**Parlamento Europeo**
2019-2024

*Comisión de Mercado Interior y Protección del Consumidor Comisión de Libertades Civiles, Justicia y Asuntos de Interior*

2.2.2024

# ACUERDO PROVISIONAL RESULTANTE DE LAS NEGOCIACIONES INTERINSTITUCIONALES

**Asunto: Propuesta de Reglamento por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Ley sobre Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión 2021/0106(COD)**
**(COM(2021)0206 - C9-0146(2021) - 2021/0106(COD))**

Las negociaciones interinstitucionales sobre la citada propuesta de Reglamento han desembocado en un compromiso. De conformidad con el apartado 4 del artículo 74 del Reglamento, el acuerdo provisional, que se reproduce a continuación, se presenta en su conjunto a la Comisión de Mercado Interior y Protección del Consumidor
Comisión de Libertades Civiles, Justicia y Asuntos de Interior para decisión en votación única.



**ES**



**ES**

**traducción automatizada con versión pro**

**dispuesta por Lorenzo Cotino**
**www.cotino.es**

**versión original en inglés en**
**https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/AG/2024/02-13/1296003EN.pdf**

ANEXO

2021/0106 (BACALAO)

Propuesta de

# REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

## POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS SOBRE INTELIGENCIA ARTIFICIAL (ACTO SOBRE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Tras la transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[1] , Visto el dictamen del Banco Central Europeo[2] ,

Visto el dictamen conjunto del Consejo Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos,

Visto el dictamen del Comité de las Regiones[3] , De conformidad con el procedimiento legislativo ordinario, Considerando lo siguiente:

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior estableciendo un marco jurídico uniforme, en particular para el desarrollo, la comercialización, la puesta en servicio y el uso de sistemas de inteligencia artificial en la Unión de conformidad con los valores de la Unión, promover la adopción de una inteligencia artificial centrada en el ser humano y digna de confianza, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad, los derechos fundamentales consagrados en la Carta, incluidos la democracia y el Estado de Derecho y la protección del medio ambiente, contra los efectos nocivos de los sistemas de inteligencia artificial en la Unión y apoyar la innovación. Este Reglamento garantiza la libre circulación transfronteriza de bienes y servicios basados en la IA, impidiendo así que los Estados miembros impongan restricciones al desarrollo, la comercialización y el uso de sistemas de inteligencia artificial (sistemas de IA), a menos que el presente Reglamento lo autorice explícitamente.

---

1 DO C [...], [...], p. [...].

2 Referencia al dictamen del BCE.

3 DO C [...], [...], p. [...].

(1 bis) El presente Reglamento debe aplicarse de conformidad con los valores de la Unión consagrados en la Carta, facilitando la protección de las personas, las empresas, la democracia y el Estado de Derecho y el medio ambiente, impulsando al mismo tiempo la innovación y el empleo y haciendo de la Unión un líder en la adopción de una IA fiable.

(2) Los sistemas de IA pueden desplegarse fácilmente en múltiples sectores de la economía y la sociedad, incluidos los transfronterizos, y circular por toda la Unión. Algunos Estados miembros ya han estudiado la adopción de normas nacionales para garantizar que la inteligencia artificial sea digna de confianza y segura y se desarrolle y utilice respetando las obligaciones en materia de derechos fundamentales. La existencia de normas nacionales diferentes puede dar lugar a la fragmentación del mercado interior y disminuir la seguridad jurídica de los operadores que desarrollan, importan o utilizan sistemas de IA. Por consiguiente, debe garantizarse un nivel de protección coherente y elevado en toda la Unión para lograr una IA digna de confianza, al tiempo que deben evitarse las divergencias que obstaculizan la libre circulación, la innovación, el despliegue y la adopción de los sistemas de IA y los productos y servicios relacionados dentro del mercado interior, estableciendo obligaciones uniformes para los operadores y garantizando la protección uniforme de las razones imperiosas de interés público y de los derechos de las personas en todo el mercado interior sobre la base del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE). En la medida en que el presente Reglamento contiene normas específicas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales relativos a las restricciones de la utilización de sistemas de IA para la identificación biométrica a distancia a efectos de la aplicación de la ley, para la utilización de sistemas de IA para la evaluación del riesgo de las personas físicas a efectos de la aplicación de la ley y para la utilización de sistemas de IA de categorización biométrica a efectos de la aplicación de la ley, procede basar el presente Reglamento, en lo que respecta a dichas normas específicas, en el artículo 16 del TFUE. A la luz de esas normas específicas y del recurso al artículo 16 del TFUE, procede consultar al Consejo Europeo de Protección de Datos.

(3) La inteligencia artificial es una familia de tecnologías en rápida evolución que contribuye a una amplia gama de beneficios económicos, medioambientales y sociales en todo el espectro de industrias y actividades sociales. Al mejorar la predicción, optimizar las operaciones y la asignación de recursos y personalizar las soluciones digitales disponibles para particulares y organizaciones, el uso de la inteligencia artificial puede proporcionar ventajas competitivas clave a las empresas y respaldar resultados beneficiosos desde el punto de vista social y medioambiental, por ejemplo en la asistencia sanitaria, la agricultura, la seguridad alimentaria, la educación y la formación, los medios de comunicación, el deporte, la cultura, la gestión de infraestructuras, la energía, el transporte y la logística, los servicios públicos y la seguridad,

justicia, eficiencia energética y de recursos, vigilancia medioambiental, conservación y restauración de la biodiversidad y los ecosistemas y mitigación del cambio climático y adaptación al mismo.

(4) Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación específica, uso y nivel de desarrollo tecnológico, la inteligencia artificial puede generar riesgos y causar daños a los intereses públicos y a los derechos fundamentales protegidos por el Derecho de la Unión. Estos daños pueden ser materiales o inmateriales, incluidos los daños físicos, psicológicos, sociales o económicos.

(4 bis) Dado el gran impacto que la inteligencia artificial puede tener en la sociedad y la necesidad de generar confianza, es vital que la inteligencia artificial y su marco regulador se desarrollen de acuerdo con los valores de la Unión consagrados en el artículo 2 del TUE, los derechos y libertades fundamentales consagrados en los Tratados y la Carta. Como requisito previo, la inteligencia artificial debe ser una tecnología centrada en el ser humano. Debe servir como herramienta para las personas, con el objetivo último de aumentar el bienestar humano.

(4aa)Para garantizar un nivel coherente y elevado de protección de los intereses públicos en materia de salud, seguridad y derechos fundamentales, deben establecerse normas comunes para todos los sistemas de IA de alto riesgo. Dichas normas deben ser coherentes con la Carta de los Derechos Fundamentales de la Unión Europea (la Carta), no discriminatorias y acordes con los compromisos comerciales internacionales de la Unión. También deberían tener en cuenta la Declaración Europea sobre Derechos y Principios Digitales para la Década Digital (2023/C 23/01) y las Directrices Éticas para una Inteligencia Artificial (IA) digna de confianza del Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial.

(5) Por consiguiente, es necesario un marco jurídico de la Unión que establezca normas armonizadas en materia de inteligencia artificial para fomentar el desarrollo, la utilización y la asimilación de la inteligencia artificial en el mercado interior que, al mismo tiempo, responda a un elevado nivel de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, tal como se reconocen y protegen en el Derecho de la Unión. Para alcanzar este objetivo, deben establecerse normas que regulen la comercialización, la puesta en servicio y la utilización de determinados sistemas de IA, garantizando así el buen funcionamiento del mercado interior y permitiendo que dichos sistemas se beneficien del principio de libre circulación de mercancías y servicios. Estas normas deben ser claras y sólidas en la protección de los derechos fundamentales, apoyar las nuevas soluciones innovadoras, permitir un ecosistema europeo de agentes públicos y privados que creen sistemas de IA en consonancia con los valores de la Unión y liberar el potencial de la transformación digital en todas las regiones de la Unión. Al establecer

Estas normas, así como las medidas de apoyo a la innovación, con especial atención a las PYME, incluidas las nuevas empresas, este Reglamento apoya el objetivo de promover el enfoque europeo de la IA centrado en el ser humano y de ser un líder mundial en el desarrollo de una inteligencia artificial segura, digna de confianza y ética, tal como declaró el Consejo Europeo[4] , y garantiza la protección de los principios éticos, tal como solicitó específicamente el Parlamento Europeo[5] .

(5 bis) Las normas armonizadas sobre comercialización, puesta en servicio y uso de los sistemas de IA establecidas en el presente Reglamento deben aplicarse en todos los sectores y, en consonancia con su enfoque de nuevo marco legislativo, deben entenderse sin perjuicio de la legislación de la Unión vigente, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo y protección de los trabajadores y seguridad de los productos, de la que el presente Reglamento es complementario. En consecuencia, no se verán afectados y serán plenamente aplicables todos los derechos y vías de recurso previstos en dicha legislación de la Unión para los consumidores y otras personas que puedan verse afectadas negativamente por los sistemas de IA, incluido lo relativo a la indemnización por posibles daños y perjuicios de conformidad con la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos. Por otra parte, en el contexto del empleo y de la protección de los trabajadores, el presente Reglamento no debe afectar, por tanto, al Derecho de la Unión en materia de política social ni al Derecho laboral nacional, de conformidad con el Derecho de la Unión, relativo al empleo y a las condiciones de trabajo, incluidas la salud y la seguridad en el trabajo y las relaciones entre empresarios y trabajadores. El presente Reglamento tampoco debe afectar al ejercicio de los derechos fundamentales reconocidos en los Estados miembros y a escala de la Unión, incluido el derecho o la libertad de huelga o de emprender otras acciones contempladas en los sistemas específicos de relaciones laborales de los Estados miembros, así como el derecho a negociar, celebrar y aplicar convenios colectivos o a emprender acciones colectivas de conformidad con la legislación nacional. [El presente Reglamento no debe afectar a las disposiciones destinadas a mejorar las condiciones de trabajo en el trabajo en plataformas establecidas en la Directiva ... [COD 2021/414/CE]]. Además, el presente Reglamento tiene por objeto reforzar la eficacia de los derechos y recursos existentes mediante el establecimiento de requisitos y obligaciones específicos, en particular en materia de transparencia, documentación técnica y registro de los sistemas de IA. Además, las obligaciones impuestas a los distintos operadores que intervienen en la cadena de valor de la IA en virtud del presente Reglamento deben aplicarse sin perjuicio de las legislaciones nacionales, en cumplimiento de

[4] Consejo Europeo, Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) - Conclusiones, EUCO 13/20, 2020, p. 6.

[5] Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012(INL).

con el Derecho de la Unión, que tengan por efecto limitar el uso de determinados sistemas de IA cuando dichas leyes queden fuera del ámbito de aplicación del presente Reglamento o persigan otros objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Por ejemplo, el Derecho laboral nacional y las leyes sobre protección de menores (es decir, personas menores de 18 años) que tengan en cuenta la Observación General nº 25 (2021) de las Naciones Unidas sobre los derechos del niño, en la medida en que no sean específicos de los sistemas de IA y persigan otros objetivos legítimos de interés público, no deben verse afectados por el presente Reglamento.

(5aa) El derecho fundamental a la protección de los datos personales está salvaguardado, en particular, por los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva 2016/680. La Directiva 2002/58/CE protege además la vida privada y la confidencialidad de las comunicaciones, incluso mediante el establecimiento de condiciones para el almacenamiento de datos personales y no personales y el acceso a ellos desde equipos terminales. Estos actos jurídicos de la Unión sientan las bases para un tratamiento de datos sostenible y responsable, incluso cuando los conjuntos de datos incluyen una mezcla de datos personales y no personales. El presente Reglamento no pretende afectar a la aplicación del Derecho de la Unión vigente que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de control independientes competentes para supervisar el cumplimiento de dichos instrumentos. Tampoco afecta a las obligaciones de los proveedores e implantadores de sistemas de IA en su papel de responsables o encargados del tratamiento derivadas del Derecho nacional o de la Unión en materia de protección de datos personales en la medida en que el diseño, el desarrollo o el uso de sistemas de IA impliquen el tratamiento de datos personales. También conviene aclarar que los interesados siguen disfrutando de todos los derechos y garantías que les otorga dicho Derecho de la Unión, incluidos los derechos relacionados únicamente con la toma de decisiones individuales automatizadas, incluida la elaboración de perfiles. Las normas armonizadas para la comercialización, la puesta en servicio y el uso de los sistemas de IA establecidos en virtud del presente Reglamento deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos de los interesados y otras vías de recurso garantizadas por el Derecho de la Unión en materia de protección de datos personales y de otros derechos fundamentales.

(5 bis) El presente Reglamento debe entenderse sin perjuicio de las disposiciones relativas a la responsabilidad de los proveedores de servicios intermediarios establecidas en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo [modificada por la Ley de Servicios Digitales].

(6) La noción de sistema de IA en el presente Reglamento debe definirse claramente y ajustarse estrechamente a la labor de las organizaciones internacionales que trabajan en el ámbito de la inteligencia artificial para garantizar la seguridad jurídica, facilitar la convergencia internacional y una amplia aceptación, proporcionando al mismo tiempo la flexibilidad necesaria para adaptarse a la rápida evolución tecnológica en este ámbito.

Además, debe basarse en las características clave de los sistemas de inteligencia artificial, que los distinguen de los sistemas de software tradicionales más sencillos o de los enfoques de programación, y no debe abarcar los sistemas que se basan en las reglas definidas únicamente por personas físicas para ejecutar operaciones automáticamente. Una característica clave de los sistemas de IA es su capacidad para inferir. Esta inferencia se refiere al proceso de obtención de resultados, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos y virtuales, y a una capacidad de los sistemas de IA para derivar modelos y/o algoritmos a partir de entradas/datos. Las técnicas que permiten la inferencia al construir un sistema de IA incluyen enfoques de aprendizaje automático que aprenden a partir de los datos cómo alcanzar determinados objetivos; y enfoques basados en la lógica y el conocimiento que infieren a partir del conocimiento codificado o la representación simbólica de la tarea que debe resolverse. La capacidad de un sistema de IA para inferir va más allá del procesamiento básico de datos, permitiendo el aprendizaje, el razonamiento o el modelado. El término "basado en máquinas" se refiere al hecho de que los sistemas de IA funcionan en máquinas. La referencia a objetivos explícitos o implícitos subraya que los sistemas de IA pueden funcionar con arreglo a objetivos explícitos definidos o a objetivos implícitos. Los objetivos del sistema de IA pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico. A efectos del presente Reglamento, los entornos deben entenderse como los contextos en los que operan los sistemas de IA, mientras que los resultados generados por el sistema de IA reflejan diferentes funciones realizadas por los sistemas de IA e incluyen predicciones, contenidos, recomendaciones o decisiones. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que tienen cierto grado de independencia de las acciones de la intervención humana y de capacidades para funcionar sin intervención humana. La capacidad de adaptación que puede mostrar un sistema de IA tras su despliegue se refiere a las capacidades de autoaprendizaje, que permiten al sistema cambiar mientras se utiliza. Los sistemas de IA pueden utilizarse de forma autónoma o como componente de un producto, independientemente de que el sistema esté integrado físicamente en el producto (integrado) o sirva a la funcionalidad del producto sin estar integrado en él (no integrado).

(6 bis) El concepto de "responsable del despliegue" a que se refiere el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida una autoridad pública, agencia u otro organismo, que utilice un sistema de IA bajo su autoridad, excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas de quien lo despliega.

(7) El concepto de datos biométricos utilizado en el presente Reglamento debe interpretarse a la luz del concepto de datos biométricos definido en el artículo 4, apartado 14, del Reglamento (UE) 2016/679 de la

Parlamento Europeo y del Consejo[6] , el artículo 3, apartado 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[7] y el artículo 3, apartado 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[8] .Los datos biométricos pueden permitir la autenticación, identificación o categorización de personas físicas y el reconocimiento de emociones de personas físicas.

(7 bis)El concepto de identificación biométrica, tal como se utiliza en el presente Reglamento, debe definirse como el reconocimiento automatizado de rasgos humanos físicos, fisiológicos y de comportamiento, como el rostro, el movimiento de los ojos, la forma del cuerpo, la voz, la prosodia, la marcha, la postura, la frecuencia cardíaca, la presión arterial, el olor, las características de las pulsaciones de teclas, con el fin de establecer la identidad de una persona mediante la comparación de los datos biométricos de dicha persona con los datos biométricos almacenados de personas físicas en una base de datos de referencia, independientemente de que la persona física haya dado o no su consentimiento. Esto excluye los sistemas de IA destinados a ser utilizados para la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física específica es la persona que dice ser y confirmar la identidad de una persona física con el único propósito de tener acceso a un servicio, desbloquear un dispositivo o tener acceso de seguridad a locales.

(7 ter) La noción de categorización biométrica utilizada en el presente Reglamento debe definirse como la asignación de personas físicas a categorías específicas sobre la base de sus datos biométricos. Dichas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos de comportamiento o de personalidad, la lengua, la religión, la pertenencia a una minoría nacional o la orientación sexual o política. Esto no incluye los sistemas de categorización biométrica que son una característica puramente auxiliar intrínsecamente vinculada a otro servicio comercial, lo que significa que la característica no puede, por razones técnicas objetivas, utilizarse sin el servicio principal y la integración de esa característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas del presente Reglamento. Por ejemplo, los filtros de categorización de rasgos faciales o corporales utilizados en los mercados en línea podrían constituir una característica accesoria de este tipo, ya que pueden

---

[6] 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) (DO L 119 de 4.5.2016, p. 1).

[7] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

[8] 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 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 estos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva sobre la aplicación de la ley) (DO L 119 de 4.5.2016, p. 89).

utilizarse únicamente en relación con el servicio principal, que consiste en vender un producto permitiendo al consumidor previsualizar la visualización del producto en sí mismo y ayudándole a tomar una decisión de compra. Los filtros utilizados en los servicios de redes sociales en línea que categorizan los rasgos faciales o corporales para permitir a los usuarios añadir o modificar imágenes o vídeos también podrían considerarse una característica accesoria, ya que dicho filtro no puede utilizarse sin el servicio principal de los servicios de redes sociales consistente en compartir contenidos en línea.

(8) La noción de sistema de identificación biométrica a distancia, tal como se utiliza en el presente Reglamento, debe definirse funcionalmente como un sistema de IA destinado a la identificación de personas físicas sin su participación activa, normalmente a distancia, mediante la comparación de los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos utilizados. Estos sistemas de identificación biométrica a distancia se utilizan normalmente para percibir simultáneamente a varias personas o su comportamiento con el fin de facilitar de forma significativa la identificación de personas físicas sin su participación activa. Esto excluye los sistemas de IA destinados a ser utilizados para la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física específica es la persona que dice ser y confirmar la identidad de una persona física con el único propósito de tener acceso a un servicio, desbloquear un dispositivo o tener acceso de seguridad a locales. Esta exclusión se justifica por el hecho de que es probable que tales sistemas tengan un impacto menor en los derechos fundamentales de las personas físicas en comparación con los sistemas de identificación biométrica a distancia, que pueden utilizarse para el tratamiento de los datos biométricos de un gran número de personas sin su participación activa. En el caso de los sistemas "en tiempo real", la captura de los datos biométricos, la comparación y la identificación se producen de forma instantánea, casi instantánea o, en cualquier caso, sin un retraso significativo. A este respecto, no debe haber margen para eludir las normas del presente Reglamento sobre el uso "en tiempo real" de los sistemas de IA en cuestión previendo retrasos menores. Los sistemas "en tiempo real" implican el uso de material "en directo" o "casi en directo", como imágenes de vídeo, generadas por una cámara u otro dispositivo con una funcionalidad similar. En cambio, en los sistemas "a posteriori", los datos biométricos ya se han capturado y la comparación y la identificación sólo se producen tras un retraso significativo. Se trata de material, como imágenes o secuencias de vídeo generadas por cámaras de circuito cerrado de televisión o dispositivos privados, que se ha generado antes de la utilización del sistema con respecto a las personas físicas en cuestión.

(8 bis) A efectos del presente Reglamento, la noción de sistema de reconocimiento de emociones debe definirse como un sistema de IA destinado a identificar o deducir emociones o intenciones.

de las personas físicas a partir de sus datos biométricos. Se refiere a emociones o intenciones como felicidad, tristeza, ira, sorpresa, asco, vergüenza, excitación, vergüenza, desprecio, satisfacción y diversión. No incluye estados físicos como el dolor o la fatiga. No se refiere, por ejemplo, a los sistemas utilizados para detectar el estado de fatiga de pilotos o conductores profesionales con el fin de prevenir accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos fácilmente aparentes, a menos que se utilicen para identificar o deducir emociones. Estas expresiones pueden ser expresiones faciales básicas, como fruncir el ceño o sonreír, o gestos, como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, por ejemplo, un tono de voz elevado o un susurro.

(9) A efectos del presente Reglamento, debe entenderse que la noción de espacio de acceso público se refiere a cualquier lugar físico que sea accesible a un número indeterminado de personas físicas, e independientemente de que el lugar en cuestión sea de propiedad privada o pública y de la actividad para la que pueda utilizarse, como el comercio (por ejemplo, tiendas, restaurantes, cafés), servicios (por ejemplo, bancos, actividades profesionales, hostelería), deporte (por ejemplo, piscinas, gimnasios, estadios), transporte (por ejemplo, estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte), ocio (por ejemplo, cines, teatros, museos, salas de conciertos y conferencias) u otros (por ejemplo, vías y plazas públicas, parques, bosques, zonas de juegos). Un lugar debe clasificarse como de acceso público también si, independientemente de las posibles restricciones de capacidad o seguridad, el acceso está sujeto a ciertas condiciones predeterminadas, que pueden cumplir un número indeterminado de personas, como la compra de un billete o título de transporte, el registro previo o tener una determinada edad. Por el contrario, un lugar no debe considerarse accesible al público si el acceso está limitado a personas físicas concretas y definidas, ya sea mediante legislación de la Unión o nacional directamente relacionada con la seguridad pública o mediante la manifestación clara de voluntad de la persona que tiene la autoridad pertinente sobre el lugar. La mera posibilidad fáctica de acceso (por ejemplo, una puerta sin cerrar, una puerta abierta en una valla) no implica que el lugar sea accesible al público en presencia de indicios o circunstancias que sugieran lo contrario (por ejemplo, señales que prohíban o restrinjan el acceso). Los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que sólo pueden acceder los empleados y proveedores de servicios pertinentes, no son lugares accesibles al público. Los espacios de acceso público no deben incluir prisiones ni controles fronterizos. Algunos otros espacios pueden estar compuestos tanto de espacios no accesibles al público como de espacios accesibles al público, como el pasillo de un edificio residencial privado necesario para acceder a la consulta de un médico o a un aeropuerto. Tampoco se incluyen los espacios en línea, ya que no son espacios físicos. Si un determinado

Sin embargo, la cuestión de si un espacio es accesible al público debe determinarse caso por caso, teniendo en cuenta las especificidades de cada situación.

(9 ter) Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y para permitir el control democrático, la alfabetización en materia de IA debe dotar a los proveedores, implantadores y personas afectadas de las nociones necesarias para tomar decisiones con conocimiento de causa en relación con los sistemas de IA. Estas nociones pueden variar en función del contexto pertinente y pueden incluir la comprensión de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar los resultados del sistema de IA y, en el caso de las personas afectadas, los conocimientos necesarios para comprender cómo les afectarán las decisiones adoptadas con la ayuda de la IA. En el contexto de la aplicación del presente Reglamento, la alfabetización en IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el adecuado cumplimiento y su correcta aplicación. Además, la aplicación generalizada de medidas de alfabetización en materia de IA y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo y, en última instancia, a sostener la consolidación y la trayectoria de innovación de una IA fiable en la Unión. La Junta Europea de Inteligencia Artificial debería apoyar a la Comisión en la promoción de herramientas de alfabetización en IA, la concienciación pública y la comprensión de los beneficios, riesgos, salvaguardias, derechos y obligaciones en relación con el uso de sistemas de IA. En cooperación con las partes interesadas pertinentes, la Comisión y los Estados miembros deberían facilitar la elaboración de códigos de conducta voluntarios para fomentar la alfabetización en materia de IA entre las personas que se ocupan del desarrollo, el funcionamiento y el uso de la IA.

(10) Para garantizar la igualdad de condiciones y una protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas por el presente Reglamento deben aplicarse a los proveedores de sistemas de IA de forma no discriminatoria, con independencia de que estén establecidos en la Unión o en un tercer país, y a los implantadores de sistemas de IA establecidos en la Unión.

(11) Habida cuenta de su naturaleza digital, determinados sistemas de IA deben entrar en el ámbito de aplicación del presente Reglamento aunque no se comercialicen, ni se pongan en servicio, ni se utilicen en la Unión. Este es el caso, por ejemplo, de un operador establecido en la Unión que contrata determinados servicios a un operador establecido fuera de la Unión en relación con una actividad que debe realizar un sistema de IA que se calificaría de alto riesgo. En tales circunstancias, el sistema de IA utilizado por el operador establecido fuera de la Unión podría tratar los datos recogidos legalmente en la Unión y transferidos desde ésta, y proporcionar al operador contratante de la Unión la producción de dicho sistema de IA resultante de ese tratamiento, sin que

que dicho sistema de IA se comercialice, se ponga en servicio o se utilice en la Unión. Para evitar que se eluda el presente Reglamento y garantizar una protección efectiva de las personas físicas establecidas en la Unión, el presente Reglamento debe aplicarse también a los proveedores e implantadores de sistemas de inteligencia artificial establecidos en un tercer país, en la medida en que los resultados producidos por dichos sistemas estén destinados a ser utilizados en la Unión. No obstante, para tener en cuenta los acuerdos existentes y las necesidades especiales de cooperación futura con socios extranjeros con los que se intercambien información y pruebas, el presente Reglamento no debe aplicarse a las autoridades públicas de un tercer país y a las organizaciones internacionales cuando actúen en el marco de acuerdos de cooperación o internacionales celebrados a nivel nacional o europeo para la aplicación de la ley y la cooperación judicial con la Unión o con sus Estados miembros, a condición de que dicho tercer país u organizaciones internacionales ofrezcan garantías adecuadas con respecto a la protección de los derechos y libertades fundamentales de las personas. En su caso, esto puede abarcar también las actividades de las entidades encargadas por los terceros países de llevar a cabo tareas específicas en apoyo de dicha cooperación policial y judicial. Tales marcos de cooperación o acuerdos se han establecido bilateralmente entre los Estados miembros y terceros países o entre la Unión Europea, Europol y otras agencias de la UE y terceros países y organizaciones internacionales. Las autoridades competentes para la supervisión de las autoridades policiales y judiciales en virtud de la Ley sobre la IA deben evaluar si estos marcos de cooperación o acuerdos internacionales incluyen garantías adecuadas con respecto a la protección de los derechos y libertades fundamentales de las personas. Las autoridades de los Estados miembros receptores y las instituciones, oficinas y organismos de la Unión que hagan uso de esos resultados en la Unión seguirán siendo responsables de garantizar que su utilización se ajusta al Derecho de la Unión. Cuando se revisen esos acuerdos internacionales o se celebren otros nuevos en el futuro, las partes contratantes deben hacer el máximo esfuerzo para adaptar dichos acuerdos a los requisitos del presente Reglamento.

(12) El presente Reglamento también debe aplicarse a las instituciones, oficinas, organismos y agencias de la Unión cuando actúen como proveedores o implantadores de un sistema de IA.

(12 bis) En la medida en que los sistemas de IA se comercialicen, se pongan en servicio o se utilicen, con o sin modificación de dichos sistemas, con fines militares, de defensa o de seguridad nacional, deben quedar excluidos del ámbito de aplicación del presente Reglamento, con independencia del tipo de entidad que lleve a cabo dichas actividades, por ejemplo, si se trata de una entidad pública o privada. Por lo que respecta a los fines militares y de defensa, dicha exclusión está justificada tanto por el artículo 4, apartado 2, del TUE como por las especificidades de la política de defensa de los Estados miembros y de la Unión común.

cubiertos por el capítulo 2 del título V del Tratado de la Unión Europea (TUE) que están sujetos al Derecho internacional público, que es, por tanto, el marco jurídico más adecuado para la regulación de los sistemas de IA en el contexto del uso de la fuerza letal y de otros sistemas de IA en el contexto de actividades militares y de defensa. Por lo que respecta a los fines de seguridad nacional, la exclusión se justifica tanto por el hecho de que la seguridad nacional sigue siendo responsabilidad exclusiva de los Estados miembros, de conformidad con el artículo 4, apartado 2, del TUE, como por la naturaleza específica y las necesidades operativas de las actividades de seguridad nacional y las normas nacionales específicas aplicables a dichas actividades. No obstante, si un sistema de IA desarrollado, comercializado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional se utiliza fuera de ellos temporal o permanentemente para otros fines (por ejemplo, fines civiles o humanitarios, policiales o de seguridad pública), dicho sistema entraría en el ámbito de aplicación del presente Reglamento. En ese caso, la entidad que utilice el sistema para fines distintos de los militares, de defensa o de seguridad nacional deberá garantizar la conformidad del sistema con el presente Reglamento, a menos que el sistema ya sea conforme con el presente Reglamento. Los sistemas de IA comercializados o puestos en servicio para un fin excluido (es decir, militar, de defensa o de seguridad nacional) y uno o más fines no excluidos (por ejemplo, fines civiles, policiales, etc.) entran en el ámbito de aplicación del presente Reglamento y los proveedores de dichos sistemas deben garantizar el cumplimiento del presente Reglamento. En estos casos, el hecho de que un sistema de IA pueda entrar en el ámbito de aplicación del presente Reglamento no debe afectar a la posibilidad de que las entidades que lleven a cabo actividades de seguridad nacional, defensa y militares, independientemente del tipo de entidad que lleve a cabo dichas actividades, utilicen sistemas de IA para fines de seguridad nacional, militares y de defensa, cuyo uso está excluido del ámbito de aplicación del presente Reglamento. Un sistema de IA comercializado con fines civiles o policiales que se utilice, con o sin modificaciones, con fines militares, de defensa o de seguridad nacional no debe entrar en el ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo dichas actividades.

(12 quater) El presente Reglamento debe apoyar la innovación, respetar la libertad de la ciencia y no menoscabar la actividad de investigación y desarrollo. Por lo tanto, es necesario excluir de su ámbito de aplicación los sistemas y modelos de IA específicamente desarrollados y puestos en servicio con el único fin de la investigación y el desarrollo científicos. Además, es necesario garantizar que el Reglamento no afecte de otro modo a la actividad de investigación y desarrollo científicos sobre sistemas o modelos de IA antes de su comercialización o puesta en servicio. Por lo que se refiere a la actividad de investigación, ensayo y desarrollo orientada al producto en relación con los sistemas o modelos de IA, las disposiciones del presente Reglamento tampoco deben aplicarse antes de que estos sistemas y

modelos que se pongan en servicio o se comercialicen. Ello se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando se comercialice o se ponga en servicio un sistema de IA que entre en el ámbito de aplicación del presente Reglamento como resultado de dicha actividad de investigación y desarrollo y de la aplicación de las disposiciones sobre los "cajones de arena" reglamentarios y las pruebas en condiciones del mundo real. Además, sin perjuicio de lo anterior en relación con los sistemas de IA específicamente desarrollados y puestos en servicio con el único fin de la investigación y el desarrollo científicos, cualquier otro sistema de IA que pueda utilizarse para la realización de cualquier actividad de investigación y desarrollo debe seguir estando sujeto a las disposiciones del presente Reglamento. En cualquier circunstancia, cualquier actividad de investigación y desarrollo debe llevarse a cabo de conformidad con las normas éticas y profesionales reconocidas para la investigación científica y debe realizarse de conformidad con la legislación aplicable de la Unión.

(14) Para introducir un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, debe seguirse un enfoque basado en el riesgo claramente definido. Ese enfoque debería adaptar el tipo y el contenido de tales normas a la intensidad y el alcance de los riesgos que pueden generar los sistemas de IA. Por lo tanto, es necesario prohibir determinadas prácticas inaceptables de inteligencia artificial, establecer requisitos para los sistemas de IA de alto riesgo y obligaciones para los operadores correspondientes, y establecer obligaciones de transparencia para determinados sistemas de IA.

(14 bis) Si bien el enfoque basado en el riesgo es la base de un conjunto proporcionado y eficaz de normas vinculantes, es importante recordar las Directrices éticas para una IA digna de confianza de 2019 elaboradas por el Grupo de Expertos de Alto Nivel sobre IA (HLEG) independiente designado por la Comisión. En esas Directrices, el HLEG desarrolló siete principios éticos no vinculantes para la IA que deberían ayudar a garantizar que la IA sea digna de confianza y éticamente sólida. Los siete principios son: agencia y supervisión humanas; solidez y seguridad técnicas; privacidad y gobernanza de datos; transparencia; diversidad, no discriminación y equidad; bienestar social y medioambiental y responsabilidad. Sin perjuicio de los requisitos jurídicamente vinculantes del presente Reglamento y de cualquier otra legislación aplicable de la Unión, estas Directrices contribuyen al diseño de una Inteligencia Artificial coherente, digna de confianza y centrada en el ser humano, en consonancia con la Carta y con los valores en los que se fundamenta la Unión. Según las Directrices del HLEG, la agencia y la supervisión humanas significan que los sistemas de IA se desarrollan y utilizan como una herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de forma que puede ser controlada y supervisada adecuadamente por los seres humanos. Solidez y seguridad técnicas significa que los sistemas de IA se desarrollan y utilizan de forma que sean sólidos en caso de problemas y resistentes frente a los intentos de alterar el uso o el funcionamiento del sistema de IA para permitir un uso ilegal por parte de los usuarios.

terceros, y minimizar los daños involuntarios. La gobernanza de la privacidad y los datos significa que los sistemas de IA se desarrollan y utilizan de conformidad con las normas vigentes sobre privacidad y protección de datos, al tiempo que procesan datos que cumplen normas estrictas en términos de calidad e integridad.

Transparencia significa que los sistemas de IA se desarrollen y utilicen de forma que permitan una trazabilidad y una explicabilidad adecuadas, al tiempo que se informa a los seres humanos de que se comunican o interactúan con un sistema de IA, así como se informa debidamente a los usuarios de las capacidades y limitaciones de ese sistema de IA y a las personas afectadas de sus derechos.

Diversidad, no discriminación y equidad significa que los sistemas de IA se desarrollan y utilizan de forma que incluyan a diversos actores y promuevan la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los impactos discriminatorios y los sesgos injustos prohibidos por el Derecho de la Unión o nacional. Bienestar social y medioambiental significa que los sistemas de IA se desarrollan y utilizan de forma sostenible y respetuosa con el medio ambiente, así como de manera que beneficien a todos los seres humanos, al tiempo que se supervisan y evalúan los impactos a largo plazo sobre el individuo, la sociedad y la democracia. La aplicación de estos principios debe traducirse, cuando sea posible, en el diseño y uso de modelos de IA. En cualquier caso, deben servir de base para la elaboración de códigos de conducta en el marco del presente Reglamento. Se anima a todas las partes interesadas, incluidas la industria, el mundo académico, la sociedad civil y las organizaciones de normalización, a tener en cuenta, según proceda, los principios éticos para el desarrollo de mejores prácticas y normas voluntarias.

(15) Aparte de los muchos usos beneficiosos de la inteligencia artificial, esa tecnología también puede utilizarse indebidamente y proporcionar herramientas novedosas y potentes para prácticas de manipulación, explotación y control social. Tales prácticas son especialmente nocivas y abusivas y deben prohibirse porque contradicen los valores de la Unión de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y los derechos fundamentales de la Unión, incluido el derecho a la no discriminación, la protección de datos y la intimidad y los derechos del niño.

(16) Las técnicas de manipulación basadas en la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados, o para engañarlas induciéndolas a tomar decisiones que subviertan y menoscaben su autonomía, su capacidad de decisión y su libre elección. La comercialización, puesta en servicio o utilización de determinados sistemas de IA con el objetivo o el efecto de distorsionar materialmente el comportamiento humano, mediante los cuales es probable que se produzcan daños significativos, en particular con repercusiones adversas suficientemente importantes en la salud física o psicológica o en los intereses financieros, son especialmente peligrosos y, por lo tanto, deben prohibirse. Dichos sistemas de IA utilizan componentes subliminales como estímulos de audio, imagen o vídeo que las personas no pueden percibir, ya que dichos estímulos escapan a la percepción humana u otros medios.

técnicas manipuladoras o engañosas que subvierten o menoscaban la autonomía, la toma de decisiones o la libre elección de las personas de formas de las que éstas no son conscientes, o incluso si son conscientes, siguen siendo engañadas o no son capaces de controlar o resistir. Esto podría verse facilitado, por ejemplo, por las interfaces máquina-cerebro o la realidad virtual, ya que permiten un mayor grado de control de los estímulos que se presentan a las personas, en la medida en que pueden distorsionar materialmente su comportamiento de forma significativamente perjudicial. Además, los sistemas de IA también pueden explotar de otro modo las vulnerabilidades de una persona o un grupo específico de personas debido a su edad, discapacidad en el sentido de la Directiva (UE) 2019/882, o una situación social o económica específica que probablemente haga que esas personas sean más vulnerables a la explotación, como las personas que viven en condiciones de extrema pobreza o las minorías étnicas o religiosas. Tales sistemas de IA pueden comercializarse, ponerse en servicio o utilizarse con el objetivo o el efecto de distorsionar materialmente el comportamiento de una persona y de una manera que cause o sea razonablemente probable que cause un daño significativo a esa u otra persona o grupos de personas, incluidos los daños que puedan acumularse con el tiempo y que, por lo tanto, deben prohibirse. La intención de distorsionar el comportamiento puede no presumirse si la distorsión resulta de factores externos al sistema de IA que escapan al control del proveedor o del implantador, es decir, factores que no pueden ser razonablemente previstos y mitigados por el proveedor o el implantador del sistema de IA. En cualquier caso, no es necesario que el proveedor o el implantador tengan la intención de causar un daño significativo, siempre que dicho daño se derive de las prácticas manipuladoras o explotadoras del sistema de IA. Las prohibiciones de tales prácticas de IA son complementarias de las disposiciones contenidas en la Directiva 2005/29/CE, en particular las prácticas comerciales desleales que causan perjuicios económicos o financieros a los consumidores están prohibidas en todas las circunstancias, independientemente de que se lleven a cabo mediante sistemas de IA o de otro modo. Las prohibiciones de prácticas manipuladoras y explotadoras del presente Reglamento no deben afectar a las prácticas lícitas en el contexto del tratamiento médico, como el tratamiento psicológico de una enfermedad mental o la rehabilitación física, cuando dichas prácticas se lleven a cabo de conformidad con la legislación y las normas médicas aplicables, por ejemplo el consentimiento explícito de las personas o de sus representantes legales. Además, las prácticas comerciales comunes y legítimas, por ejemplo en el ámbito de la publicidad, que sean conformes con la legislación aplicable no deben considerarse en sí mismas constitutivas de prácticas manipuladoras nocivas de la IA.

(16 bis) Sistemas de categorización biométrica que se basan en datos biométricos de las personas, como la cara o la huella dactilar de una persona, para deducir o inferir las opiniones políticas, la afiliación sindical, las creencias religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona.

debe prohibirse. Esta prohibición no abarca el etiquetado, filtrado o categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho de la Unión o nacional en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o de los ojos, que puede utilizarse, por ejemplo, en el ámbito policial.

(17) Los sistemas de IA que proporcionan una puntuación social de las personas físicas por parte de agentes públicos o privados pueden dar lugar a resultados discriminatorios y a la exclusión de determinados grupos. Pueden violar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia. Estos sistemas de IA evalúan o clasifican a las personas físicas o a grupos de ellas basándose en múltiples datos relacionados con su comportamiento social en múltiples contextos o características personales o de personalidad conocidas, inferidas o predichas a lo largo de determinados periodos de tiempo. La puntuación social obtenida de tales sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de personas físicas o grupos enteros de éstas en contextos sociales que no guardan relación con el contexto en el que se generaron o recopilaron originalmente los datos, o a un trato perjudicial desproporcionado o injustificado en relación con la gravedad de su comportamiento social. Por lo tanto, deben prohibirse los sistemas de IA que conlleven tales prácticas de puntuación inaceptables que conduzcan a tales resultados perjudiciales o desfavorables. Esta prohibición no debe afectar a las prácticas lícitas de evaluación de personas físicas realizadas con un fin específico de conformidad con el Derecho nacional y de la Unión.

(18) El uso de sistemas de IA para la identificación biométrica remota "en tiempo real" de personas físicas en espacios de acceso público con fines policiales es especialmente intrusivo para los derechos y libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de gran parte de la población, evocar una sensación de vigilancia constante y disuadir indirectamente del ejercicio de la libertad de reunión y otros derechos fundamentales. Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica a distancia de personas físicas pueden dar lugar a resultados sesgados y conllevar efectos discriminatorios. Esto es especialmente relevante cuando se trata de la edad, la etnia, la raza, el sexo o las discapacidades. Además, la inmediatez del impacto y las limitadas oportunidades de realizar comprobaciones o correcciones posteriores en relación con el uso de tales sistemas que funcionan en "tiempo real" conllevan mayores riesgos para los derechos y libertades de las personas a las que afectan las actividades policiales.

(19) Por lo tanto, debe prohibirse el uso de estos sistemas con fines policiales, salvo en situaciones enumeradas exhaustivamente y definidas con precisión, en las que el uso sea estrictamente necesario para lograr un interés público sustancial, cuya importancia supere los riesgos. Dichas situaciones incluyen la búsqueda de determinadas víctimas de delitos, incluidas las personas desaparecidas; determinadas amenazas para la vida o la seguridad física de personas físicas o de un atentado terrorista; y la localización o identificación

de los autores o sospechosos de los delitos contemplados en el anexo II bis si dichos delitos son punibles en el Estado miembro de que se trate con una pena privativa de libertad o una medida de seguridad privativa de libertad de una duración máxima de al menos cuatro años y tal como se definen en la legislación de dicho Estado miembro. Este umbral para la pena privativa de libertad o la medida de seguridad de conformidad con la legislación nacional contribuye a garantizar que el delito sea lo suficientemente grave como para justificar potencialmente el uso de sistemas de identificación biométrica a distancia "en tiempo real". Por otra parte, la lista de delitos a que se refiere el anexo II bis se basa en los 32 delitos enumerados en la Decisión marco 2002/584/JAI del Consejo[9] , teniendo en cuenta que en la práctica es probable que algunos sean más pertinentes que otros, en el sentido de que el recurso a la identificación biométrica a distancia "en tiempo real" será previsiblemente necesario y proporcionado en grados muy diversos para la persecución práctica de la localización o identificación de un autor o sospechoso de los distintos delitos enumerados y habida cuenta de las diferencias probables en la gravedad, probabilidad y escala del daño o de las posibles consecuencias negativas.

Una amenaza inminente para la vida o la seguridad física de las personas físicas también podría derivarse de una perturbación grave de las infraestructuras críticas, tal como se definen en el artículo 2, letra a), de la Directiva 2008/114/CE, cuando la perturbación o destrucción de dichas infraestructuras críticas diera lugar a una amenaza inminente para la vida o la seguridad física de una persona, incluso a través de un perjuicio grave para el abastecimiento básico de la población o para el ejercicio de la función esencial del Estado.

Además, el presente Reglamento debe preservar la capacidad de las autoridades policiales, de control fronterizo, de inmigración o de asilo para llevar a cabo controles de identidad en presencia de la persona de que se trate, de conformidad con las condiciones establecidas en el Derecho de la Unión y nacional para dichos controles. En particular, las autoridades policiales, de control fronterizo, de inmigración o de asilo deben poder utilizar los sistemas de información, de conformidad con el Derecho de la Unión o nacional, para identificar a una persona que, durante un control de identidad, se niegue a ser identificada o no pueda declarar o probar su identidad, sin que el presente Reglamento le exija obtener una autorización previa. Puede tratarse, por ejemplo, de una persona implicada en un delito, que no quiera o no pueda, debido a un accidente o a un problema médico, revelar su identidad a las autoridades policiales.

---

(20) Para garantizar que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en cada una de esas situaciones exhaustivamente enumeradas y estrictamente definidas, deben tenerse en cuenta determinados elementos, en particular por lo que respecta a la naturaleza de la situación que da lugar a la solicitud y a las consecuencias de la utilización para los derechos y libertades de todas las personas afectadas, así como a las salvaguardias y condiciones previstas con la utilización. Además, el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales

[9] Decisión marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1).

sólo debe desplegarse para confirmar la identidad de la persona a la que se dirige específicamente y debe limitarse a lo estrictamente necesario en cuanto al período de tiempo y al ámbito geográfico y personal, teniendo en cuenta en particular las pruebas o indicios relativos a las amenazas, las víctimas o el autor. La utilización del sistema de identificación biométrica a distancia "en tiempo real" en espacios de acceso público sólo debe autorizarse si la autoridad policial ha realizado una evaluación de impacto sobre los derechos fundamentales y, salvo disposición en contrario del presente Reglamento, ha registrado el sistema en la base de datos tal como se establece en el presente Reglamento. La base de datos de referencia de personas debe ser adecuada para cada caso de uso en cada una de las situaciones mencionadas anteriormente.

(21) Toda utilización de un sistema de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales debe estar sujeta a una autorización expresa y específica de una autoridad judicial o de una autoridad administrativa independiente cuya decisión sea vinculante para un Estado miembro. En principio, dicha autorización deberá obtenerse antes de la utilización del sistema con vistas a identificar a una o varias personas. Deben permitirse excepciones a esta norma en situaciones de urgencia debidamente justificadas, es decir, situaciones en las que la necesidad de utilizar los sistemas en cuestión sea tal que resulte efectiva y objetivamente imposible obtener una autorización antes de comenzar la utilización. En tales situaciones de urgencia, el uso debe limitarse al mínimo absolutamente necesario y estar sujeto a las salvaguardias y condiciones apropiadas, determinadas en la legislación nacional y especificadas en el contexto de cada caso individual de uso urgente por la propia autoridad policial. Además, en tales situaciones, las fuerzas y cuerpos de seguridad deberán solicitar dicha autorización y exponer las razones por las que no han podido solicitarla antes, sin demoras indebidas y, a más tardar, en un plazo de 24 horas. Si se deniega dicha autorización, el uso de sistemas de identificación biométrica en tiempo real vinculado a dicha autorización debe interrumpirse con efecto inmediato y todos los datos relacionados con dicho uso deben descartarse y borrarse. Dichos datos incluyen los datos de entrada adquiridos directamente por un sistema de IA en el curso de la utilización de dicho sistema, así como los resultados y productos de la utilización vinculada a dicha autorización. No deben incluirse los datos de entrada adquiridos legalmente de conformidad con otra legislación nacional o de la Unión. En cualquier caso, ninguna decisión que produzca un efecto jurídico adverso sobre un

persona puede tomarse basándose únicamente en el resultado del sistema de identificación biométrica a distancia.

(21 bis)Para llevar a cabo sus tareas de conformidad con los requisitos establecidos en el presente Reglamento, así como en las normas nacionales, la autoridad de vigilancia del mercado pertinente y la autoridad nacional de protección de datos deben ser notificadas de cada uso del "sistema de identificación biométrica en tiempo real". Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos que hayan sido notificadas deben presentar a la Comisión un informe anual sobre el uso de los "sistemas de identificación biométrica en tiempo real".

(22) Además, conviene prever, en el marco exhaustivo establecido por el presente Reglamento, que dicho uso en el territorio de un Estado miembro de conformidad con el presente Reglamento sólo sea posible cuando y en la medida en que el Estado miembro en cuestión haya decidido prever expresamente la posibilidad de autorizar dicho uso en sus disposiciones de Derecho interno. Por consiguiente, los Estados miembros siguen siendo libres, en virtud del presente Reglamento, de no prever en absoluto dicha posibilidad o de preverla únicamente respecto de algunos de los objetivos que pueden justificar una utilización autorizada identificados en el presente Reglamento. Estas normas nacionales deben notificarse a la Comisión a más tardar 30 días después de su adopción.

(23) El uso de sistemas de IA para la identificación biométrica remota "en tiempo real" de personas físicas en espacios de acceso público con fines policiales implica necesariamente el tratamiento de datos biométricos. Las normas del presente Reglamento que prohíben, salvo determinadas excepciones, dicho uso, que se basan en el artículo 16 del TFUE, deben aplicarse como lex specialis respecto de las normas sobre el tratamiento de datos biométricos contenidas en el artículo 10 de la Directiva (UE) 2016/680, regulando así de manera exhaustiva dicho uso y el tratamiento de los datos biométricos implicados. Por consiguiente, dicho uso y tratamiento solo debe ser posible en la medida en que sea compatible con el marco establecido por el presente Reglamento, sin que exista margen, fuera de dicho marco, para que las autoridades competentes, cuando actúen con fines policiales, utilicen dichos sistemas y traten dichos datos en relación con ellos por los motivos enumerados en el artículo 10 de la Directiva (UE) 2016/680. En este contexto, el presente Reglamento no tiene por objeto proporcionar la base jurídica para el tratamiento de datos personales con arreglo al artículo 8 de la Directiva 2016/680. Sin embargo, el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines distintos de los policiales, incluso por parte de las autoridades competentes, no debe estar cubierto por el marco específico relativo a dicho uso con fines policiales establecido por el presente Reglamento. Por consiguiente, dicha utilización con fines distintos de los policiales no debe estar sujeta al requisito de autorización.

en virtud del presente Reglamento y de las disposiciones de Derecho interno que puedan aplicarlo.

(24) Todo tratamiento de datos biométricos y otros datos personales que conlleve el uso de sistemas de IA para la identificación biométrica, que no esté relacionado con el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales, tal como se regula en el presente Reglamento, debe seguir cumpliendo todos los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680. Para fines distintos de la aplicación de la ley, 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, salvo las excepciones limitadas previstas en dichos artículos. En aplicación del artículo 9, apartado 1, del Reglamento (UE) 2016/679, el uso de la identificación biométrica a distancia para fines distintos de la aplicación de la ley ya ha sido objeto de decisiones de prohibición por parte de las autoridades nacionales de protección de datos.

(25) De conformidad con el artículo 6 bis del Protocolo nº 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al TUE y al TFUE, Irlanda no está vinculada por las normas establecidas en el artículo 5, apartado 1, letra d), apartados 2, 3, 3 bis, 4 y 5, el artículo 5, apartado 1, letra b bis), en la medida en que se aplica a la utilización de sistemas de clasificación biométrica para actividades en el ámbito de la cooperación policial y judicial en materia penal, el artículo 5, apartado 1, letra d bis), en la medida en que se aplique a la utilización de los sistemas de inteligencia artificial contemplados en dicha disposición y en el artículo 29, apartado 6 bis, del presente Reglamento adoptado sobre la base del artículo 16 del TFUE, que se refieran al tratamiento de datos personales por los Estados miembros en el ejercicio de actividades comprendidas en el ámbito de aplicación del capítulo 4 o del capítulo 5 del título V de la tercera parte del TFUE, cuando Irlanda no esté vinculada por las normas que regulan las formas de cooperación judicial en materia penal o de cooperación policial que exigen el cumplimiento de las disposiciones establecidas sobre la base del artículo 16 del TFUE.

(26) De conformidad con los artículos 2 y 2 bis del Protocolo nº 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no está vinculada por las normas establecidas en el artículo 5, apartado 1, letras d), 2), 3), 3 bis), 4) y 5), el artículo 5, apartado 1, letra b bis), en la medida en que se aplica a la utilización de sistemas de clasificación biométrica para actividades en el ámbito de la cooperación policial y judicial en materia penal, el artículo 5, apartado 1, letra d bis), en la medida en que se aplique a la utilización de los sistemas de IA contemplados en dicha disposición y en el artículo 29, apartado 6 bis, del presente Reglamento adoptados sobre la base del artículo 16 del TFUE, o sujetos a su aplicación, que se refieran a la

el tratamiento de datos personales por los Estados miembros en el ejercicio de actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE.

(26 bis) En consonancia con la presunción de inocencia, las personas físicas en la UE deben ser juzgadas siempre por su comportamiento real. Las personas físicas nunca deben ser juzgadas por su comportamiento previsto por la IA basado únicamente en su perfil, rasgos de personalidad o características, como nacionalidad, lugar de nacimiento, lugar de residencia, número de hijos, deudas, su tipo de coche, sin una sospecha razonable de que esa persona esté implicada en una actividad delictiva basada en hechos objetivos verificables y sin una evaluación humana de la misma. Por lo tanto, deben prohibirse las evaluaciones del riesgo de las personas físicas con el fin de evaluar el riesgo de que delincan o para predecir la comisión de un delito real o potencial basándose únicamente en el perfil de una persona física o en la evaluación de sus rasgos y características de personalidad. En cualquier caso, esta prohibición no se refiere ni afecta a los análisis de riesgos que no se basan en la elaboración de perfiles de personas físicas o en los rasgos y características de la personalidad de las personas físicas, como los sistemas de IA que utilizan análisis de riesgos para evaluar el riesgo de fraude financiero por parte de las empresas sobre la base de transacciones sospechosas o las herramientas de análisis de riesgos para predecir la probabilidad de localización de estupefacientes o mercancías ilícitas por parte de las autoridades aduaneras, por ejemplo sobre la base de rutas de tráfico conocidas.

(26 ter) Debe prohibirse la comercialización, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial a través de la extracción no selectiva de imágenes faciales de Internet o de grabaciones de CCTV, ya que esta práctica aumenta la sensación de vigilancia masiva y puede dar lugar a graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad.

(26c) Existen serias dudas sobre la base científica de los sistemas de IA que pretenden identificar o inferir emociones, sobre todo porque la expresión de las emociones varía considerablemente entre culturas y situaciones, e incluso dentro de un mismo individuo. Entre las principales deficiencias de estos sistemas se encuentran su escasa fiabilidad, su falta de especificidad y su limitada generalizabilidad. Por lo tanto, los sistemas de IA que identifican o infieren emociones o intenciones de personas físicas sobre la base de sus datos biométricos pueden dar lugar a resultados discriminatorios y pueden ser intrusivos para los derechos y libertades de las personas afectadas. Teniendo en cuenta el desequilibrio de poder en el contexto del trabajo o la educación, combinado con la naturaleza intrusiva de estos sistemas, tales sistemas podrían conducir a un trato perjudicial o desfavorable de determinadas personas físicas o grupos enteros de ellas. Por consiguiente, debe prohibirse la comercialización, puesta en servicio o utilización de sistemas de IA destinados a detectar el estado emocional de las personas en situaciones relacionadas con el trabajo y la educación. Esta prohibición no debe

cubren los sistemas de IA comercializados estrictamente por razones médicas o de seguridad, como los sistemas destinados a uso terapéutico.

(26 quinquies) El presente Reglamento no debe afectar a las prácticas prohibidas por la legislación de la Unión, incluida la legislación sobre protección de datos, no discriminación, protección de los consumidores y competencia.

(27) Los sistemas de IA de alto riesgo solo deben introducirse en el mercado de la Unión, ponerse en servicio o utilizarse si cumplen determinados requisitos obligatorios. Estos requisitos deben garantizar que los sistemas de IA de alto riesgo disponibles en la Unión o cuyos resultados se utilicen de otro modo en la Unión no planteen riesgos inaceptables para los intereses públicos importantes de la Unión reconocidos y protegidos por el Derecho de la Unión. Siguiendo el enfoque del nuevo marco legislativo, como se aclara en la Comunicación de la Comisión "Guía azul" sobre la aplicación de las normas de la UE sobre productos 2022 (C/2022/3637), la norma general es que varios actos legislativos de la UE, como el Reglamento (UE) 2017/745 sobre productos sanitarios y el Reglamento (UE) 2017/746 sobre productos para diagnóstico in vitro o la Directiva 2006/42/CE sobre máquinas, pueden tener que tomarse en consideración para un producto, ya que la puesta a disposición o la puesta en servicio solo pueden tener lugar cuando el producto cumple toda la legislación de armonización de la Unión aplicable. Para garantizar la coherencia y evitar cargas o costes administrativos innecesarios, los proveedores de un producto que contenga uno o varios sistemas de inteligencia artificial de alto riesgo, al que se apliquen los requisitos del presente Reglamento, así como los requisitos de la legislación de armonización de la Unión enumerados en el anexo II, sección A, deben disponer de flexibilidad en las decisiones operativas sobre cómo garantizar de la mejor manera posible la conformidad de un producto que contenga uno o varios sistemas de inteligencia artificial con todos los requisitos aplicables de la legislación armonizada de la Unión. Los sistemas de IA identificados como de alto riesgo deben limitarse a aquellos que tengan un impacto perjudicial significativo en la salud, la seguridad y los derechos fundamentales de las personas en la Unión y dicha limitación minimice cualquier posible restricción al comercio internacional, si la hubiera.

(28) Los sistemas de IA podrían tener repercusiones negativas para la salud y la seguridad de las personas, en particular cuando dichos sistemas funcionan como componentes de seguridad de los productos. En consonancia con los objetivos de la legislación de armonización de la Unión de facilitar la libre circulación de productos en el mercado interior y garantizar que solo los productos seguros y conformes en otros aspectos encuentren su camino en el mercado, es importante que los riesgos de seguridad que pueda generar un producto en su conjunto debido a sus componentes digitales, incluidos los sistemas de IA, se prevengan y mitiguen debidamente. Por ejemplo, los robots cada vez más autónomos, ya sea en el contexto de la fabricación o de la asistencia y los cuidados personales, deben ser capaces de operar con seguridad y desempeñar sus funciones en entornos complejos. Del mismo modo, en el sector sanitario, donde la

Los riesgos para la vida y la salud son especialmente elevados, por lo que los sistemas de diagnóstico cada vez más sofisticados y los sistemas de apoyo a las decisiones humanas deben ser fiables y precisos.

(28 bis)El alcance del impacto adverso causado por el sistema de IA sobre los derechos fundamentales protegidos por la Carta es de especial relevancia a la hora de clasificar un sistema de IA como de alto riesgo. Estos derechos incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos personales, la libertad de expresión e información, la libertad de reunión y de asociación, y la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas con discapacidad, la igualdad de género, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, el derecho de defensa y la presunción de inocencia, el derecho a una buena administración. Además de estos derechos, es importante destacar que los niños tienen derechos específicos consagrados en el artículo 24 de la Carta de la UE y en la Convención de las Naciones Unidas sobre los Derechos del Niño (desarrollados en la Observación General nº 25 de la CNUDN por lo que se refiere al entorno digital), que exigen tener en cuenta la vulnerabilidad de los niños y proporcionarles la protección y los cuidados necesarios para su bienestar. El derecho fundamental a un alto nivel de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión también debe tenerse en cuenta a la hora de evaluar la gravedad del daño que puede causar un sistema de IA, incluso en relación con la salud y la seguridad de las personas.

(29) Por lo que respecta a los sistemas de IA de alto riesgo que son componentes de seguridad de productos o sistemas, o que son en sí mismos productos o sistemas incluidos en el ámbito de aplicación del Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo[10] , el Reglamento (UE) nº 167/2013 del Parlamento Europeo y del Consejo[11] , Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo[12] , Directiva 2014/90/UE del Parlamento Europeo y del Consejo[13] , Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo[14] , Reglamento (UE) 2018/858 del Parlamento Europeo y del

[10] Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) nº 2320/2002 (DO L 97 de 9.4.2008, p. 72).

[11] Reglamento (UE) nº 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos agrícolas y forestales (DO L 60 de 2.3.2013, p. 1).

[12] Reglamento (UE) nº 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos de dos o tres ruedas y los cuatriciclos (DO L 60 de 2.3.2013, p. 52).

[13] Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos y por la que se deroga la Directiva 96/98/CE del Consejo (DO L 257 de 28.8.2014, p. 146).

[14] Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea (DO L 138 de 26.5.2016, p. 44).

Consejo15, el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo16, y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo17, procede modificar dichos actos para garantizar que la Comisión tenga en cuenta, sobre la base de las especificidades técnicas y reglamentarias de cada sector, y sin interferir con los mecanismos y autoridades de gobernanza, evaluación de la conformidad y ejecución existentes establecidos en ellos, los requisitos obligatorios para los sistemas de IA de alto riesgo establecidos en el presente Reglamento cuando adopte cualquier futuro acto delegado o de ejecución pertinente sobre la base de dichos actos.

(30) Por lo que respecta a los sistemas de IA que son componentes de seguridad de productos, o que son en sí mismos productos, que entran en el ámbito de aplicación de determinada legislación de armonización de la Unión enumerada en el anexo II, procede clasificarlos como de alto riesgo con arreglo al presente Reglamento si el producto en cuestión se somete al procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad de terceros con arreglo a dicha legislación de armonización de la Unión pertinente. En particular, tales productos son las máquinas, los juguetes, los ascensores, los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas, los equipos radioeléctricos, los equipos a presión, los equipos para embarcaciones de recreo, las instalaciones de transporte por cable, los aparatos de gas, los productos sanitarios y los productos sanitarios para diagnóstico in vitro.

(31) La clasificación de un sistema de IA como de alto riesgo con arreglo al presente Reglamento no debe significar necesariamente que el producto cuyo componente de seguridad sea el sistema de IA, o el propio sistema de IA como producto, se considere de "alto riesgo" con arreglo a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto. Este es, en particular, el caso del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo**[18]** y

**[15]** Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1).

**[16]** Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea y se modifican los Reglamentos (CE) n.o 2111/2005, (CE) n.o 1008/2008, (UE) n.o 996/2010, (UE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo, y por el que se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo (DO L 212 de 22.8.2018, p. 1).

**[17]** Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, sobre los requisitos de homologación de tipo para los vehículos de motor y sus remolques, y los sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, en lo relativo a su seguridad general y a la protección de los ocupantes de vehículos y los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 78/2009, (CE) nº 79/2009 y (CE) nº 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010 de la Comisión, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012 y (UE) 2015/166 (DO L 325 de 16.12.2019, p. 1).

**[18]** Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios,

Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo[19] , en el que se prevé una evaluación de la conformidad por terceros para los productos de riesgo medio y alto.

(32) Por lo que se refiere a los sistemas de IA autónomos, es decir, los sistemas de IA de alto riesgo distintos de los que son componentes de seguridad de productos, o que son ellos mismos productos, procede clasificarlos como de alto riesgo si, a la luz de su finalidad prevista, plantean un alto riesgo de daño para la salud y la seguridad o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible daño como su probabilidad de ocurrencia, y se utilizan en una serie de ámbitos predefinidos específicamente que se especifican en el Reglamento. La identificación de esos sistemas se basa en la misma metodología y criterios previstos también para cualquier modificación futura de la lista de sistemas de IA de alto riesgo que la Comisión debe estar facultada para adoptar, mediante actos delegados, a fin de tener en cuenta el rápido ritmo del desarrollo tecnológico, así como los posibles cambios en el uso de los sistemas de IA.

(32 bis) También es importante aclarar que puede haber casos específicos en los que los sistemas de IA referidos a ámbitos predefinidos especificados en el presente Reglamento no den lugar a un riesgo significativo de perjuicio de los intereses jurídicos protegidos en dichos ámbitos, porque no influyan materialmente en la toma de decisiones o no perjudiquen sustancialmente dichos intereses. A efectos del presente Reglamento, por sistema de IA que no influye materialmente en el resultado de la toma de decisiones debe entenderse un sistema de IA que no incide en el fondo, y por tanto en el resultado, de la toma de decisiones, ya sea humana o automatizada. Este podría ser el caso si se cumplen una o más de las siguientes condiciones. El primer criterio debe ser que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada, como un sistema de IA que transforme datos no estructurados en datos estructurados, un sistema de IA que clasifique documentos entrantes en categorías o un sistema de IA que se utilice para detectar duplicados entre un gran número de aplicaciones. Estas tareas son de naturaleza tan estrecha y limitada que sólo plantean riesgos limitados que no aumentan por el uso en un contexto enumerado en el anexo III. El segundo criterio debe ser que la tarea realizada por el sistema de IA esté destinada a mejorar el resultado de una actividad humana realizada previamente que pueda ser relevante para la

finalidad del caso de uso enumerado en el anexo III. Teniendo en cuenta estas características, el sistema de IA sólo proporciona una capa adicional a una actividad humana con el consiguiente menor riesgo. Por ejemplo, este criterio se aplicaría a los sistemas de IA destinados a mejorar la

---

por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

[19] Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios para diagnóstico in vitro y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176).

lenguaje utilizado en documentos redactados previamente, por ejemplo en relación con el tono profesional, el estilo académico del lenguaje o alineando el texto con un determinado mensaje de marca. El tercer criterio debe ser que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones de patrones de toma de decisiones anteriores. El riesgo se reduciría porque el uso del sistema de IA sigue a una evaluación humana realizada previamente, a la que no pretende sustituir ni influir, sin una revisión humana adecuada. Estos sistemas de IA incluyen, por ejemplo, los que, dado un determinado patrón de calificación de un profesor, pueden utilizarse para comprobar a posteriori si el profesor puede haberse desviado del patrón de calificación, con el fin de señalar posibles incoherencias o anomalías. El cuarto criterio debe ser que el sistema de IA esté destinado a realizar una tarea que sólo sea preparatoria para una evaluación pertinente a efectos del caso de uso enumerado en el anexo III, con lo que el posible impacto del resultado del sistema será muy bajo en términos de representar un riesgo para la evaluación posterior. Por ejemplo, este criterio abarca soluciones inteligentes para el tratamiento de archivos, que incluyen diversas funciones de indexación, búsqueda, tratamiento de texto y voz o vinculación de datos a otras fuentes de datos, o sistemas de IA utilizados para la traducción de documentos iniciales. En cualquier caso, debe considerarse que los sistemas de IA mencionados en el anexo III plantean riesgos significativos de daño para la salud, la seguridad o los derechos fundamentales de las personas físicas si el sistema de IA implica la elaboración de perfiles en el sentido del artículo 4, apartado 4, del Reglamento (UE) 2016/679 y del artículo 3, apartado 4, de la Directiva (UE) 2016/680 y del artículo 3, apartado 5, del Reglamento 2018/1725. Para garantizar la trazabilidad y la transparencia, el proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto riesgo sobre la base de los criterios mencionados debe elaborar la documentación de la evaluación antes de que dicho sistema se comercialice o se ponga en servicio, y debe facilitar dicha documentación a las autoridades nacionales competentes a petición de estas. Dicho proveedor debe estar obligado a registrar el sistema en la base de datos de la UE establecida en virtud del presente Reglamento. Con vistas a proporcionar más orientaciones para la aplicación práctica de los criterios con arreglo a los cuales los sistemas de IA mencionados en el anexo III no son excepcionalmente de alto riesgo, la Comisión, previa consulta al Consejo de IA, debe proporcionar directrices que especifiquen esta aplicación práctica, completadas con una lista exhaustiva de ejemplos prácticos de casos de uso de alto riesgo y de no alto riesgo de los sistemas de IA.

(33 bis) Dado que los datos biométricos constituyen una categoría especial de datos personales sensibles, procede clasificar como de alto riesgo varios casos críticos de utilización de sistemas biométricos, en la medida en que su uso esté permitido por el Derecho nacional y de la Unión pertinente. Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica a distancia de personas físicas pueden dar lugar a resultados sesgados y conllevar efectos discriminatorios. Esto es especialmente relevante cuando se trata de la edad,

etnia, raza, sexo o discapacidad. Por lo tanto, los sistemas de identificación biométrica a distancia deben clasificarse como de alto riesgo en vista de los riesgos que plantean. Esto excluye los sistemas de IA destinados a ser utilizados para la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física específica es la persona que dice ser y confirmar la identidad de una persona física con el único propósito de tener acceso a un servicio, desbloquear un dispositivo o tener acceso seguro a locales.

Además, los sistemas de IA destinados a utilizarse para la categorización biométrica con arreglo a atributos o características sensibles protegidos en virtud del artículo 9, apartado 1, del Reglamento (UE) 2016/679 basados en datos biométricos, en la medida en que no estén prohibidos en virtud del presente Reglamento, y los sistemas de reconocimiento de emociones que no estén prohibidos en virtud del presente Reglamento, deben clasificarse como de alto riesgo. No deben considerarse sistemas de alto riesgo los sistemas biométricos destinados a ser utilizados únicamente con el fin de habilitar medidas de ciberseguridad y protección de datos personales.

(34) Por lo que respecta a la gestión y el funcionamiento de las infraestructuras críticas, procede clasificar como de alto riesgo los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas enumeradas en el anexo I, punto 8, de la Directiva sobre la resiliencia de las entidades críticas, el tráfico por carretera y el suministro de agua, gas, calefacción y electricidad, ya que su fallo o mal funcionamiento puede poner en peligro la vida y la salud de las personas a gran escala y provocar perturbaciones apreciables en el desarrollo ordinario de las actividades sociales y económicas. Los componentes de seguridad de las infraestructuras críticas, incluidas las infraestructuras digitales críticas, son sistemas utilizados para proteger directamente la integridad física de las infraestructuras críticas o la salud y la seguridad de las personas y los bienes, pero que no son necesarios para que el sistema funcione. El fallo o mal funcionamiento de tales componentes podría provocar directamente riesgos para la integridad física de las infraestructuras críticas y, por tanto, riesgos para la salud y la seguridad de las personas y los bienes. Los componentes destinados a ser utilizados únicamente con fines de ciberseguridad no deben considerarse componentes de seguridad. Ejemplos de componentes de seguridad de tales infraestructuras críticas pueden ser los sistemas de control de la presión del agua o los sistemas de control de alarmas contra incendios en centros de computación en nube.

(35) El despliegue de sistemas de IA en la educación es importante para promover una educación y formación digitales de alta calidad y para permitir que todos los alumnos y profesores adquieran y compartan las habilidades y competencias digitales necesarias, incluida la alfabetización mediática, y el pensamiento crítico, para participar activamente en la economía, la sociedad y los procesos democráticos. Sin embargo, los sistemas de IA utilizados en la educación o la formación profesional, en particular para determinar el acceso o la admisión, para asignar personas a instituciones educativas y de formación profesional o

Los programas de todos los niveles, para evaluar los resultados del aprendizaje de las personas, para evaluar el nivel de educación adecuado para una persona e influir materialmente en el nivel de educación y formación que las personas recibirán o al que podrán acceder, o para controlar y detectar comportamientos prohibidos de los alumnos durante las pruebas, deben clasificarse como sistemas de IA de alto riesgo, ya que pueden determinar el curso educativo y profesional de la vida de una persona y, por tanto, afectar a su capacidad para asegurarse el sustento. Cuando se diseñan y utilizan de forma inadecuada, estos sistemas pueden ser especialmente intrusivos y vulnerar el derecho a la educación y a la formación, así como el derecho a no ser discriminado, y perpetuar pautas históricas de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, personas con discapacidad o personas de determinados orígenes raciales o étnicos u orientación sexual.

(36) Los sistemas de IA utilizados en el empleo, la gestión de trabajadores y el acceso al trabajo por cuenta propia, en particular para la contratación y selección de personas, para la toma de decisiones que afectan a las condiciones de la relación laboral, la promoción y la finalización de relaciones contractuales relacionadas con el trabajo, para la asignación de tareas basadas en el comportamiento individual, los rasgos o características personales y para el seguimiento o la evaluación de las personas en relaciones contractuales relacionadas con el trabajo, también deben clasificarse como de alto riesgo, ya que estos sistemas pueden tener un impacto apreciable en las perspectivas futuras de carrera, los medios de subsistencia de estas personas y los derechos de los trabajadores. Las relaciones contractuales pertinentes relacionadas con el trabajo deben incluir de manera significativa a los empleados y a las personas que prestan servicios a través de plataformas, tal como se menciona en el Programa de Trabajo 2021 de la Comisión. A lo largo del proceso de contratación y en la evaluación, promoción o retención de personas en relaciones contractuales relacionadas con el trabajo, estos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, personas con discapacidad o personas de determinados orígenes raciales o étnicos u orientación sexual. Los sistemas de IA utilizados para controlar el rendimiento y el comportamiento de estas personas también pueden menoscabar sus derechos fundamentales a la protección de datos y a la intimidad.

(37) Otro ámbito en el que el uso de sistemas de IA merece una consideración especial es el acceso y disfrute de determinados servicios y prestaciones públicas y privadas esenciales necesarios para que las personas participen plenamente en la sociedad o mejoren su nivel de vida. En particular, las personas físicas que solicitan o reciben prestaciones y servicios esenciales de asistencia pública de las autoridades públicas, a saber, servicios de asistencia sanitaria, prestaciones de la seguridad social, servicios sociales que proporcionan protección en casos tales como maternidad, enfermedad, accidentes laborales, dependencia o vejez y pérdida del empleo y ayudas sociales y para la vivienda, suelen depender de dichas prestaciones y servicios y se encuentran en una posición vulnerable en relación con las autoridades responsables. Si se utilizan sistemas de IA para determinar si tales prestaciones y servicios

deben ser concedidas, denegadas, reducidas, revocadas o reclamadas por las autoridades, incluida la cuestión de si los beneficiarios tienen derecho legítimo a tales prestaciones o servicios, esos sistemas pueden tener un impacto significativo en los medios de subsistencia de las personas y pueden vulnerar sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a un recurso efectivo, por lo que deben clasificarse como de alto riesgo. No obstante, el presente Reglamento no debe obstaculizar el desarrollo y la utilización de enfoques innovadores en la administración pública, que podría beneficiarse de un uso más amplio de sistemas de IA conformes y seguros, siempre que dichos sistemas no entrañen un riesgo elevado para las personas físicas y jurídicas. Además, los sistemas de IA utilizados para evaluar la puntuación crediticia o la solvencia de las personas físicas deben clasificarse como sistemas de IA de alto riesgo, ya que determinan el acceso de esas personas a recursos financieros o a servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones. Los sistemas de IA utilizados con este fin pueden dar lugar a la discriminación de personas o grupos y perpetuar pautas históricas de discriminación, por ejemplo por motivos de origen racial o étnico, sexo, discapacidad, edad u orientación sexual, o crear nuevas formas de impacto discriminatorio. No obstante, los sistemas de IA previstos por el Derecho de la Unión con fines de detección del fraude en la oferta de servicios financieros y con fines prudenciales para calcular los requisitos de capital de las entidades de crédito y las empresas de seguros no deben considerarse de alto riesgo con arreglo al presente Reglamento. Por otra parte, los sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas para los seguros de salud y de vida también pueden tener un impacto significativo en los medios de vida de las personas y, si no se diseñan, desarrollan y utilizan debidamente, pueden vulnerar sus derechos fundamentales y acarrear graves consecuencias para la vida y la salud de las personas, incluida la exclusión financiera y la discriminación. Por último, los sistemas de IA utilizados para evaluar y clasificar las llamadas de emergencia de personas físicas o para despachar o establecer la prioridad en el despacho de los servicios de primera respuesta de emergencia, incluidos los de policía, bomberos y ayuda médica, así como de los sistemas de triaje de pacientes de asistencia sanitaria de emergencia, también deben clasificarse como de alto riesgo, ya que toman decisiones en situaciones muy críticas para la vida y la salud de las personas y sus bienes.

(38) Habida cuenta de su función y responsabilidad, las actuaciones de las fuerzas y cuerpos de seguridad que implican determinados usos de los sistemas de IA se caracterizan por un importante grado de desequilibrio de poder y pueden dar lugar a la vigilancia, detención o privación de libertad de una persona física, así como a otras repercusiones negativas sobre los derechos fundamentales garantizados en la Carta. En particular, si el sistema de IA no se entrena con datos de alta calidad, no cumple los requisitos adecuados en cuanto a su rendimiento, su precisión o robustez, o no se diseña y prueba adecuadamente antes de su comercialización o puesta en servicio por otros medios, puede señalar a personas de forma

de manera discriminatoria o incorrecta o injusta. Además, el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como el derecho de defensa y la presunción de inocencia, podría verse obstaculizado, en particular, cuando dichos sistemas de IA no sean suficientemente transparentes, explicables y documentados. Por consiguiente, procede clasificar como de alto riesgo, en la medida en que su uso esté permitido por el Derecho nacional y de la Unión pertinente, una serie de sistemas de IA destinados a ser utilizados en el contexto policial, en el que la exactitud, la fiabilidad y la transparencia son especialmente importantes para evitar repercusiones negativas, conservar la confianza de los ciudadanos y garantizar la rendición de cuentas y la reparación efectiva. Habida cuenta de la naturaleza de las actividades en cuestión y de los riesgos conexos, estos sistemas de IA de alto riesgo deben incluir, en particular, los sistemas de IA destinados a ser utilizados por las autoridades policiales o en su nombre o por los organismos, oficinas u órganos de la Unión en apoyo de las autoridades policiales para evaluar el riesgo de que una persona física sea víctima de infracciones penales, como los polígrafos y herramientas similares , para la evaluación de la fiabilidad de las pruebas en el curso de la investigación o el enjuiciamiento de delitos y, en la medida en que no esté prohibido por el presente Reglamento, para evaluar el riesgo de que una persona física delinca o reincida, sin basarse únicamente en la elaboración de perfiles de personas físicas ni en la evaluación de rasgos y características de la personalidad o del comportamiento delictivo anterior de personas físicas o grupos, para la elaboración de perfiles en el curso de la detección, investigación o enjuiciamiento de delitos, . Los sistemas de IA destinados específicamente a ser utilizados en procedimientos administrativos por las autoridades tributarias y aduaneras, así como por las unidades de inteligencia financiera que lleven a cabo tareas administrativas de análisis de la información con arreglo a la legislación de la Unión contra el blanqueo de capitales, no deben clasificarse como sistemas de IA de alto riesgo utilizados por las fuerzas y cuerpos de seguridad a efectos de prevención, detección, investigación y enjuiciamiento de infracciones penales. El uso de herramientas de IA por parte de las fuerzas y cuerpos de seguridad y las autoridades no debe convertirse en un factor de desigualdad o exclusión. No deben ignorarse las repercusiones del uso de herramientas de IA en los derechos de defensa de los sospechosos, en particular la dificultad para obtener información significativa sobre el funcionamiento de estos sistemas y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas investigadas.

(39) Los sistemas de IA utilizados en la gestión de la migración, el asilo y el control de fronteras afectan a personas que a menudo se encuentran en una situación especialmente vulnerable y que dependen del resultado de las actuaciones de las autoridades públicas competentes. La exactitud, el carácter no discriminatorio y la transparencia de los sistemas de IA utilizados en esos contextos son, por tanto, especialmente importantes para garantizar el respeto de los derechos fundamentales de las personas afectadas, en particular de sus

los derechos a la libre circulación, la no discriminación, la protección de la vida privada y de los datos personales, la protección internacional y la buena administración. Por consiguiente, procede clasificar como de alto riesgo, en la medida en que su uso esté permitido en virtud del Derecho de la Unión y nacional pertinente, los sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o por las agencias, oficinas u organismos de la Unión encargados de tareas en los ámbitos de la gestión de la migración, el asilo y el control de fronteras, o en su nombre, como polígrafos e instrumentos similares, para evaluar determinados riesgos que presentan las personas físicas que entran en el territorio de un Estado miembro o solicitan visado o asilo, para asistir a las autoridades públicas competentes en el examen, incluida la correspondiente evaluación de la fiabilidad de las pruebas, de las solicitudes de asilo, visado y permisos de residencia y las reclamaciones conexas con el objetivo de determinar la admisibilidad de las personas físicas que solicitan un estatuto, a efectos de detectar, reconocer o identificar a personas físicas en el contexto de la gestión de la migración, el asilo y el control fronterizo, con excepción de los documentos de viaje. Los sistemas de IA en el ámbito de la gestión de la migración, el asilo y el control fronterizo cubiertos por el presente Reglamento deben cumplir los requisitos de procedimiento pertinentes establecidos por la Directiva 2013/32/UE del Parlamento Europeo y del Consejo[20] , el Reglamento (CE) nº 810/2009 del Parlamento Europeo y del Consejo[21] y demás legislación pertinente. Los Estados miembros o las instituciones, agencias u organismos de la Unión no deben utilizar en ningún caso los sistemas de IA en la gestión de la migración, el asilo y el control de fronteras como medio para eludir sus obligaciones internacionales en virtud de la Convención sobre el Estatuto de los Refugiados de 28 de julio de 1951, modificada por el Protocolo de 31 de enero de 1967, ni para infringir en modo alguno el principio de no devolución, ni para denegar vías legales seguras y efectivas de entrada en el territorio de la Unión, incluido el derecho a la protección internacional.

(40) Determinados sistemas de IA destinados a la administración de justicia y a los procesos democráticos deben clasificarse como de alto riesgo, teniendo en cuenta su impacto potencialmente significativo en la democracia, el Estado de Derecho, las libertades individuales, así como el derecho a un recurso efectivo y a un juicio justo. En particular, para hacer frente a los riesgos de posibles sesgos, errores y opacidad, conviene calificar de alto riesgo los sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para asistir a las autoridades judiciales en la investigación e interpretación de los hechos y de la ley y en la aplicación de la ley a un conjunto concreto de hechos. También deben considerarse de alto riesgo los sistemas de IA destinados a ser utilizados por entidades de resolución alternativa de litigios para estos fines.

---

[20] Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para conceder o retirar la protección internacional (DO L 180 de 29.6.2013, p. 60).

[21] Reglamento (CE) nº 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre Visados (Código sobre Visados) (DO L 243 de 15.9.2009, p. 1).

cuando los resultados de los procedimientos de resolución alternativa de litigios producen efectos jurídicos para las partes. El uso de herramientas de inteligencia artificial puede respaldar el poder de decisión de los jueces o la independencia judicial, pero no debe sustituirlo, ya que la toma de decisiones final debe seguir siendo una actividad y una decisión humanas. Esta calificación no debe extenderse, sin embargo, a los sistemas de IA destinados a actividades administrativas puramente auxiliares que no afectan a la administración real de justicia en casos individuales, como la anonimización o seudonimización de decisiones judiciales, documentos o datos, comunicación entre personal, tareas administrativas.

(40 bis) Sin perjuicio de las normas previstas en el [Reglamento xxx sobre la transparencia y la orientación de la publicidad política], y con el fin de abordar los riesgos de interferencia externa indebida en el derecho de voto consagrado en el artículo 39 de la Carta, y de efectos adversos en la democracia y el Estado de Derecho, los sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referendos deben clasificarse como sistemas de IA de alto riesgo, con la excepción de los sistemas de IA a cuyo resultado no están expuestas directamente las personas físicas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico.

(41) El hecho de que un sistema de IA esté clasificado como sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como una indicación de que el uso del sistema es lícito en virtud de otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión, como los relativos a la protección de datos personales, al uso de polígrafos y herramientas similares u otros sistemas para detectar el estado emocional de las personas físicas. Cualquier uso de este tipo debe seguir produciéndose únicamente de conformidad con los requisitos aplicables derivados de la Carta y de los actos aplicables del Derecho derivado de la Unión y del Derecho nacional. No debe entenderse que el presente Reglamento establece el fundamento jurídico para el tratamiento de datos personales, incluidas las categorías especiales de datos personales, en su caso, a menos que se disponga específicamente lo contrario en el presente Reglamento.

(42) Para mitigar los riesgos de los sistemas de inteligencia artificial de alto riesgo comercializados o puestos en servicio y garantizar un alto nivel de fiabilidad, deben aplicarse determinados requisitos obligatorios a los sistemas de inteligencia artificial de alto riesgo, teniendo en cuenta la finalidad prevista y el contexto de uso del sistema de inteligencia artificial y de acuerdo con el sistema de gestión de riesgos que establezca el proveedor. Las medidas adoptadas por los proveedores para cumplir los requisitos obligatorios del presente Reglamento deben tener en cuenta el estado de la técnica generalmente reconocido en materia de inteligencia artificial, ser proporcionadas y eficaces para cumplir los objetivos de

el presente Reglamento. Siguiendo el enfoque del nuevo marco legislativo, tal como se aclara en la Comunicación de la Comisión titulada "Guía azul" sobre la aplicación de las normas de la UE relativas a los productos de 2022 (C/2022/3637), la norma general es que para un producto pueden tener que tomarse en consideración varios actos legislativos de la UE, ya que la puesta a disposición o la puesta en servicio solo pueden tener lugar cuando el producto cumple toda la legislación de armonización de la Unión aplicable. Los peligros de los sistemas de IA cubiertos por los requisitos del presente Reglamento se refieren a aspectos diferentes de los de los actos de armonización de la Unión vigentes y, por lo tanto, los requisitos del presente Reglamento complementarían el corpus actual de los actos de armonización de la Unión.

Por ejemplo, los productos de maquinaria o productos sanitarios que incorporan un sistema de IA podrían presentar riesgos no contemplados por los requisitos esenciales de salud y seguridad establecidos en la legislación armonizada pertinente de la Unión, ya que esta legislación sectorial no aborda los riesgos específicos de los sistemas de IA. Esto exige una aplicación simultánea y complementaria de los distintos actos legislativos. Para garantizar la coherencia y evitar cargas o costes administrativos innecesarios, los proveedores de un producto que contenga uno o varios sistemas de inteligencia artificial de alto riesgo, al que se apliquen los requisitos del presente Reglamento, así como los requisitos de la legislación de armonización de la Unión enumerados en el anexo II, sección A, deben disponer de flexibilidad en las decisiones operativas sobre cómo garantizar el cumplimiento de un producto que contenga uno o varios sistemas de inteligencia artificial con todos los requisitos aplicables de la legislación armonizada de la Unión de la mejor manera posible. Esta flexibilidad podría significar, por ejemplo, la decisión del proveedor de integrar una parte de los procesos necesarios de ensayo y notificación, información y documentación exigidos en virtud del presente Reglamento en la documentación y los procedimientos ya existentes exigidos en virtud de la legislación de armonización de la Unión vigente enumerada en el anexo II, sección A. No obstante, esto no debe menoscabar en modo alguno la obligación del proveedor de cumplir todos los requisitos aplicables.

(42 bis) El sistema de gestión de riesgos debe consistir en un proceso continuo e iterativo que se planifique y ejecute a lo largo de todo el ciclo de vida de un sistema de IA de alto riesgo. Este proceso debe tener por objeto identificar y mitigar los riesgos pertinentes de los sistemas de inteligencia artificial para la salud, la seguridad y los derechos fundamentales. El sistema de gestión de riesgos debe revisarse y actualizarse periódicamente para garantizar su eficacia permanente, así como la justificación y documentación de todas las decisiones y acciones significativas adoptadas con arreglo al presente Reglamento. Este proceso debe garantizar que el proveedor identifique los riesgos o impactos adversos y aplique medidas de mitigación de los riesgos conocidos y razonablemente previsibles de los sistemas de inteligencia artificial para la salud, la seguridad y los derechos fundamentales a la luz de su finalidad prevista y del uso indebido razonablemente previsible, incluidos los posibles riesgos

derivados de la interacción entre el sistema de IA y el entorno en el que opera. El sistema de gestión de riesgos debe adoptar las medidas de gestión de riesgos más adecuadas a la luz del estado de la técnica en materia de IA. A la hora de identificar las medidas de gestión de riesgos más adecuadas, el proveedor debe documentar y explicar las opciones elegidas y, cuando proceda, implicar a expertos y partes interesadas externas. Al identificar el uso indebido razonablemente previsible de los sistemas de IA de alto riesgo, el proveedor deberá cubrir los usos de los sistemas de IA que, aunque no estén directamente cubiertos por la finalidad prevista y contemplados en las instrucciones de uso, puedan, no obstante, esperarse razonablemente como resultado de un comportamiento humano fácilmente previsible en el contexto de las características específicas y del uso del sistema de IA concreto. Cualquier circunstancia conocida o previsible, relacionada con el uso del sistema de IA de alto riesgo de conformidad con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales debe incluirse en las instrucciones de uso facilitadas por el proveedor. Con ello se pretende garantizar que el usuario las conozca y las tenga en cuenta al utilizar el sistema de IA de alto riesgo. La identificación y aplicación de medidas de mitigación de riesgos para usos indebidos previsibles con arreglo al presente Reglamento no debe requerir medidas de formación adicionales específicas para el sistema de IA de alto riesgo por parte del proveedor para abordarlas. No obstante, se anima a los proveedores a considerar tales medidas de formación adicionales para mitigar los usos indebidos razonablemente previsibles, según resulte necesario y adecuado.

(43) Deben aplicarse requisitos a los sistemas de IA de alto riesgo en lo que respecta a la gestión de riesgos, la calidad y pertinencia de los conjuntos de datos utilizados, la documentación técnica y el mantenimiento de registros, la transparencia y el suministro de información a los usuarios, la supervisión humana, y la solidez, precisión y ciberseguridad. Estos requisitos son necesarios para mitigar eficazmente los riesgos para la salud, la seguridad y los derechos fundamentales, y no se dispone razonablemente de otras medidas menos restrictivas del comercio, evitando así restricciones injustificadas al comercio.

(44) Los datos de alta calidad y el acceso a datos de alta calidad desempeñan un papel vital a la hora de proporcionar estructura y garantizar el rendimiento de muchos sistemas de IA, especialmente cuando se utilizan técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funcione según lo previsto y de forma segura y no se convierta en una fuente de discriminación prohibida por el Derecho de la Unión. Los conjuntos de datos de alta calidad para el entrenamiento, la validación y las pruebas requieren la aplicación de prácticas adecuadas de gobernanza y gestión de datos. Los conjuntos de datos para la formación, la validación y las pruebas, incluidas las etiquetas, deben ser pertinentes, suficientemente representativos y, en la medida de lo posible, libres de errores y completos en vista de la finalidad prevista del sistema. Para facilitar el cumplimiento de la protección de datos de la UE

la legislación, como el Reglamento (UE) 2016/679, las prácticas de gobernanza y gestión de datos deben incluir, en el caso de los datos personales, la transparencia sobre la finalidad original de la recopilación de datos, Los conjuntos de datos también deben tener las propiedades estadísticas adecuadas, incluso en lo que respecta a las personas o grupos de personas en relación con los cuales está previsto utilizar el sistema de IA de alto riesgo, prestando especial atención a la mitigación de posibles sesgos en los conjuntos de datos, que puedan afectar a la salud y la seguridad de las personas, repercutir negativamente en los derechos fundamentales o dar lugar a discriminaciones prohibidas por el Derecho de la Unión, especialmente cuando los resultados de los datos influyan en las entradas para futuras operaciones ("bucles de retroalimentación") . Los sesgos pueden, por ejemplo, ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, o generarse cuando los sistemas se aplican en entornos del mundo real. Los resultados proporcionados por los sistemas de IA podrían verse influidos por tales sesgos inherentes, que tienden a aumentar gradualmente y, por tanto, a perpetuar y amplificar la discriminación existente, en particular para las personas pertenecientes a determinados grupos vulnerables, incluidos los grupos raciales o étnicos. El requisito de que los conjuntos de datos sean, en la medida de lo posible, completos y estén libres de errores no debe afectar al uso de técnicas de preservación de la intimidad en el contexto del desarrollo y las pruebas de los sistemas de IA. En particular, los conjuntos de datos deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos propios del entorno geográfico, contextual, conductual o funcional específico en el que se pretende utilizar el sistema de IA. Los requisitos relativos a la gobernanza de los datos pueden cumplirse recurriendo a terceros que ofrezcan servicios certificados de conformidad, incluida la verificación de la gobernanza de los datos, la integridad de los conjuntos de datos y las prácticas de formación, validación y ensayo de datos, en la medida en que se garantice el cumplimiento de los requisitos relativos a los datos del presente Reglamento.

(45) Para el desarrollo y la evaluación de los sistemas de IA de alto riesgo, determinados agentes, como los proveedores, los organismos notificados y otras entidades pertinentes, como los centros de innovación digital, las instalaciones de experimentación de ensayos y los investigadores, deben poder acceder y utilizar conjuntos de datos de alta calidad en sus respectivos ámbitos de actividad relacionados con el presente Reglamento. Los espacios comunes europeos de datos establecidos por la Comisión y la facilitación del intercambio de datos entre empresas y con la administración en interés público serán fundamentales para proporcionar un acceso fiable, responsable y no discriminatorio a datos de alta calidad para la formación, validación y ensayo de sistemas de IA. Por ejemplo, en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a los datos sanitarios y el entrenamiento de los algoritmos de inteligencia artificial en esos conjuntos de datos, de manera que se preserve la privacidad y sea seguro, oportuno, transparente y fiable, y con un marco institucional adecuado.

gobernanza. Las autoridades competentes pertinentes, incluidas las sectoriales, que faciliten o apoyen el acceso a los datos también podrán apoyar el suministro de datos de alta calidad para la formación, validación y prueba de los sistemas de IA.

(45 bis) El derecho a la intimidad y a la protección de los datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar el cumplimiento de dichos principios pueden incluir no solo la anonimización y el cifrado, sino también el uso de tecnología que permita llevar algoritmos a los datos y permita el entrenamiento de los sistemas de IA sin la transmisión entre las partes o la copia de los propios datos en bruto o estructurados, sin perjuicio de los requisitos sobre gobernanza de datos previstos en el presente Reglamento.

(44 quater)Con el fin de proteger el derecho de los demás frente a la discriminación que podría derivarse del sesgo en los sistemas de IA, los proveedores deben, excepcionalmente, en la medida en que sea estrictamente necesario para garantizar la detección y corrección de sesgos en relación con 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 establecidas en virtud del presente Reglamento, además de las condiciones establecidas en el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725,poder tratar también categorías especiales de datos personales, como una cuestión de interés público sustancial 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.

(46) Disponer de información comprensible sobre cómo se han desarrollado los sistemas de IA de alto riesgo y cómo funcionan a lo largo de su vida útil es esencial para permitir la trazabilidad de dichos sistemas, verificar el cumplimiento de los requisitos del presente Reglamento, así como el seguimiento de sus operaciones y la supervisión posterior a la comercialización. Para ello es necesario mantener registros y disponer de una documentación técnica que contenga la información necesaria para evaluar la conformidad del sistema de IA con los requisitos pertinentes y facilitar el seguimiento posterior a la comercialización. Dicha información debe incluir las características generales, las capacidades y las limitaciones del sistema, los algoritmos, los datos, la formación, las pruebas y los procesos de validación utilizados, así como la documentación sobre el sistema de gestión de riesgos pertinente y elaborada de forma clara y completa. La documentación técnica debe mantenerse actualizada, de forma adecuada, durante toda la vida útil del sistema de IA. Además,

Los sistemas de IA de alto riesgo deben permitir técnicamente el registro automático de eventos (logs) durante toda la vida útil del sistema.

(47) Para abordar las preocupaciones relacionadas con la opacidad y la complejidad de determinados sistemas de IA y ayudar a los implantadores a cumplir sus obligaciones en virtud del presente Reglamento, debe exigirse transparencia a los sistemas de IA de alto riesgo antes de su comercialización o puesta en servicio. Los sistemas de IA de alto riesgo deben diseñarse de manera que los implantadores puedan entender cómo funciona el sistema de IA, evaluar su funcionalidad y comprender sus puntos fuertes y sus limitaciones. Los sistemas de IA de alto riesgo deben ir acompañados de la información adecuada en forma de instrucciones de uso. Dicha información debe incluir las características, capacidades y limitaciones de funcionamiento del sistema de IA. Dichas instrucciones incluirán información sobre las posibles circunstancias conocidas y previsibles relacionadas con el uso del sistema de IA de alto riesgo, incluida la actuación del usuario que pueda influir en el comportamiento y el rendimiento del sistema, en las que el sistema de IA pueda provocar riesgos para la salud, la seguridad y los derechos fundamentales, sobre los cambios que hayan sido predeterminados y cuya conformidad haya sido evaluada por el proveedor y sobre las medidas de supervisión humana pertinentes, incluidas las medidas para facilitar la interpretación de los resultados del sistema de IA por parte de los usuarios. La transparencia, incluidas las instrucciones de uso adjuntas, debe ayudar a los usuarios a utilizar el sistema y a tomar decisiones con conocimiento de causa. Entre otras cosas, los usuarios deben estar en mejores condiciones de elegir correctamente el sistema que pretenden utilizar a la luz de las obligaciones que les incumben, recibir información sobre los usos previstos y excluidos, y utilizar el sistema de IA correctamente y según proceda. Para mejorar la legibilidad y accesibilidad de la información incluida en las instrucciones de uso, cuando proceda, deben incluirse ejemplos ilustrativos, por ejemplo sobre las limitaciones y sobre los usos previstos y excluidos del sistema de IA. Los proveedores deben velar por que toda la documentación, incluidas las instrucciones de uso, contenga información significativa, completa, accesible y comprensible, teniendo en cuenta las necesidades y los conocimientos previsibles de los destinatarios del despliegue. Las instrucciones de uso deben estar disponibles en una lengua fácilmente comprensible para los destinatarios, según determine el Estado miembro de que se trate.

(48) Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de forma que las personas físicas puedan supervisar su funcionamiento, garantizar que se utilizan según lo previsto y que sus impactos se abordan a lo largo del ciclo de vida del sistema. Para ello, el proveedor del sistema deberá determinar las medidas de supervisión humana adecuadas antes de su comercialización o puesta en servicio. En particular, cuando proceda, dichas medidas deben garantizar que el sistema esté sujeto a limitaciones operativas incorporadas que no puedan ser

que el propio sistema pueda anularla y que responda al operador humano, y que las personas físicas a las que se haya asignado la supervisión humana tengan la competencia, la formación y la autoridad necesarias para desempeñar esa función. También es esencial, según proceda, garantizar que los sistemas de IA de alto riesgo incluyan mecanismos para guiar e informar a la persona física a la que se haya asignado la supervisión humana para que tome decisiones con conocimiento de causa sobre si debe intervenir, cuándo y cómo hacerlo para evitar consecuencias negativas o riesgos, o detener el sistema si no funciona según lo previsto. Teniendo en cuenta las importantes consecuencias para las personas en caso de coincidencias incorrectas por parte de determinados sistemas de identificación biométrica, conviene establecer un requisito reforzado de supervisión humana para dichos sistemas, de modo que el responsable de la aplicación no pueda adoptar ninguna medida o decisión sobre la base de la identificación resultante del sistema a menos que ésta haya sido verificada y confirmada por separado por al menos dos personas físicas. Dichas personas podrán pertenecer a una o varias entidades e incluir a la persona que opere o utilice el sistema. Este requisito no debería suponer una carga o un retraso innecesarios y podría bastar con que las verificaciones por separado de las distintas personas se registraran automáticamente en los registros generados por el sistema. Dadas las especificidades de los ámbitos de la aplicación de la ley, la migración, el control fronterizo y el asilo, este requisito no debería aplicarse en los casos en que la legislación de la Unión o nacional considere desproporcionada la aplicación de este requisito.

(49) Los sistemas de IA de alto riesgo deben funcionar de forma coherente a lo largo de su ciclo de vida y alcanzar un nivel adecuado de precisión, solidez y ciberseguridad, a la luz de su finalidad prevista y de conformidad con el estado de la técnica generalmente reconocido. Se anima a la Comisión y a las organizaciones y partes interesadas pertinentes a que tengan debidamente en cuenta la mitigación de los riesgos y las repercusiones negativas del sistema de IA. El nivel esperado de las métricas de rendimiento debe declararse en las instrucciones de uso adjuntas. Se insta a los proveedores a comunicar esta información a los usuarios de forma clara y fácilmente comprensible, sin malentendidos ni declaraciones engañosas. La legislación de la UE sobre metrología legal, incluidas la Directiva sobre instrumentos de medida (MID) y la Directiva sobre instrumentos de pesaje de funcionamiento no automático (NAWI), tiene por objeto garantizar la exactitud de las mediciones y contribuir a la transparencia y equidad de las transacciones comerciales. En este contexto, en cooperación con las partes interesadas y las organizaciones pertinentes, como las autoridades de metrología y evaluación comparativa, la Comisión debe fomentar, según proceda, el desarrollo de evaluaciones comparativas y metodologías de medición para los sistemas de IA. Al hacerlo, la Comisión debería tomar nota y colaborar con los socios internacionales que trabajan en metrología e indicadores de medición pertinentes relativos a la inteligencia artificial.

La solidez técnica es un requisito clave para los sistemas de IA de alto riesgo. Deben ser resistentes en relación con los comportamientos nocivos o indeseables que puedan derivarse de las limitaciones de los sistemas o del entorno en el que operan (por ejemplo, errores, fallos, incoherencias, situaciones inesperadas). Por lo tanto, deben adoptarse medidas técnicas y organizativas para garantizar la solidez de los sistemas de IA de alto riesgo, por ejemplo diseñando y desarrollando soluciones técnicas adecuadas para prevenir o minimizar los comportamientos nocivos o indeseables. Dichas soluciones técnicas pueden incluir, por ejemplo, mecanismos que permitan al sistema interrumpir su funcionamiento de forma segura (planes a prueba de fallos) en presencia de determinadas anomalías o cuando el funcionamiento tenga lugar fuera de ciertos límites predeterminados. La falta de protección contra estos riesgos podría tener repercusiones en la seguridad o afectar negativamente a los derechos fundamentales, por ejemplo debido a decisiones erróneas o resultados equivocados o sesgados generados por el sistema de IA.

(50) La ciberseguridad desempeña un papel crucial a la hora de garantizar que los sistemas de IA sean resistentes a los intentos de alterar su uso, comportamiento y rendimiento, o de comprometer sus propiedades de seguridad por parte de terceros malintencionados que exploten las vulnerabilidades del sistema. Los ciberataques contra los sistemas de IA pueden aprovechar activos específicos de la IA, como conjuntos de datos de entrenamiento (por ejemplo, envenenamiento de datos) o modelos entrenados (por ejemplo, ataques de adversarios o inferencia de miembros), o explotar vulnerabilidades en los activos digitales del sistema de IA o en la infraestructura de TIC subyacente. Para garantizar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas, como controles de seguridad, teniendo también en cuenta, en su caso, la infraestructura de TIC subyacente.

(51 bis) Sin perjuicio de los requisitos relacionados con la robustez y la precisión establecidos en el presente Reglamento, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento 2022/0272, de conformidad con el artículo 8 del Reglamento 2022/0272, podrán demostrar el cumplimiento del requisito de ciberseguridad del presente Reglamento mediante el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en el artículo 10 y en el anexo I del Reglamento 2022/0272.Cuando los sistemas de IA de alto riesgo cumplan los requisitos esenciales del Reglamento 2022/0272, deben considerarse conformes con los requisitos de ciberseguridad establecidos en el presente Reglamento en la medida en que la consecución de dichos requisitos se demuestre en la declaración UE de conformidad o en partes de la misma expedida con arreglo al Reglamento 2022/0272. A tal fin, la evaluación de los riesgos de ciberseguridad, asociados a un producto con elementos digitales clasificados como sistema de IA de alto riesgo con arreglo al presente Reglamento, realizada en virtud del Reglamento 2022/0272, debe considerar los riesgos para la resiliencia cibernética de un sistema de IA en lo que respecta a los intentos de terceros no autorizados de alterar su uso, comportamiento o rendimiento,

incluidas las vulnerabilidades específicas de la IA, como el envenenamiento de datos o los ataques de adversarios, así como, en su caso, los riesgos para los derechos fundamentales, tal como exige el presente Reglamento. El procedimiento de evaluación de la conformidad previsto en el presente Reglamento debe aplicarse en relación con los requisitos esenciales de ciberseguridad de un producto con elementos digitales cubierto por el Reglamento 2022/0272 y clasificado como sistema de IA de alto riesgo con arreglo al presente Reglamento. Sin embargo, esta norma no debe dar lugar a una reducción del nivel de garantía necesario para los productos críticos con elementos digitales cubiertos por el Reglamento 2022/0272. Por lo tanto, no obstante lo dispuesto en esta norma, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del presente Reglamento y que también estén calificados como productos importantes y críticos con elementos digitales con arreglo al Reglamento 2022/0272 y a los que se aplique el procedimiento de evaluación de la conformidad basado en el control interno a que se refiere el anexo VI del presente Reglamento, estarán sujetos a las disposiciones de evaluación de la conformidad del Reglamento 2022/0272 en lo que respecta a los requisitos esenciales de ciberseguridad del Reglamento 2022/0272. En este caso, para todos los demás aspectos cubiertos por el presente Reglamento deben aplicarse las disposiciones respectivas sobre evaluación de la conformidad basada en el control interno establecidas en el anexo VI del presente Reglamento. Basándose en los conocimientos y la experiencia de la ENISA sobre la política de ciberseguridad y las tareas asignadas a la ENISA en virtud del Reglamento 2019/1020, la Comisión Europea debe cooperar con la ENISA en cuestiones relacionadas con la ciberseguridad de los sistemas de IA.

(51) Como parte de la legislación de armonización de la Unión, las normas aplicables a la comercialización, la puesta en servicio y el uso de sistemas de IA de alto riesgo deben establecerse de forma coherente con el Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo[22] por el que se establecen los requisitos de acreditación y vigilancia del mercado de los productos, la Decisión nº 768/2008/CE del Parlamento Europeo y del Consejo[23] sobre un marco común para la comercialización de los productos y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo[24] sobre la vigilancia del mercado y la conformidad de los productos ("Nuevo marco legislativo para la comercialización de los productos").

(52) Conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad de la comercialización o puesta en servicio de un sistema de IA de alto riesgo,

[22] Reglamento (CE) nº 765/2008 del Parlamento Europeo 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 y por el que se deroga el Reglamento (CEE) nº 339/93 (DO L 218 de 13.8.2008, p. 30).

[23] Decisión nº 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 y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82).

[24] Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre vigilancia del mercado y conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011 (Texto pertinente a efectos del EEE) (DO L 169 de 25.6.2019, p. 1-44).

independientemente de que dicha persona física o jurídica sea la persona que diseñó o desarrolló el sistema.

(53 bis) Como signatarios de la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad (CNUDPD), la Unión y los Estados miembros están jurídicamente obligados a proteger a las personas con discapacidad contra la discriminación y a promover su igualdad, a velar por que las personas con discapacidad tengan acceso, en igualdad de condiciones con las demás, a las tecnologías y sistemas de la información y las comunicaciones, y a garantizar el respeto de la intimidad de las personas con discapacidad.

Dada la importancia y el uso crecientes de los sistemas de IA, la aplicación de los principios de diseño universal a todas las nuevas tecnologías y servicios debe garantizar el acceso pleno y en igualdad de condiciones de todas las personas potencialmente afectadas por las tecnologías de IA o que las utilicen, incluidas las personas con discapacidad, de una manera que tenga plenamente en cuenta su dignidad y diversidad inherentes. Por lo tanto, es esencial que los Proveedores garanticen el pleno cumplimiento de los requisitos de accesibilidad, incluidas la Directiva (UE) 2016/2102 y la Directiva (UE) 2019/882. Los Proveedores deben garantizar el cumplimiento de estos requisitos mediante el diseño. Por lo tanto, las medidas necesarias deben integrarse en la medida de lo posible en el diseño del sistema de IA de alto riesgo.

(53) El proveedor debe establecer un sistema de gestión de la calidad sólido, garantizar la realización del procedimiento de evaluación de la conformidad requerido, elaborar la documentación pertinente y establecer un sistema sólido de seguimiento poscomercialización. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad en virtud de la legislación sectorial pertinente de la Unión deben tener la posibilidad de incluir los elementos del sistema de gestión de la calidad previstos en el presente Reglamento como parte del sistema de gestión de la calidad existente previsto en esa otra legislación sectorial de la Unión. La complementariedad entre el presente Reglamento y el Derecho sectorial de la Unión vigente también debe tenerse en cuenta en las futuras actividades de normalización u orientaciones que adopte la Comisión. Las autoridades públicas que pongan en servicio sistemas de IA de alto riesgo para su propio uso podrán adoptar y aplicar las normas del sistema de gestión de la calidad como parte del sistema de gestión de la calidad adoptado a nivel nacional o regional, según proceda, teniendo en cuenta las especificidades del sector y las competencias y la organización de la autoridad pública de que se trate.

(56) Para permitir la aplicación del presente Reglamento y crear condiciones de igualdad para los operadores, y teniendo en cuenta las diferentes formas de puesta a disposición de productos digitales, es importante garantizar que, en cualquier circunstancia, una persona establecida en la Unión pueda facilitar a las autoridades toda la información necesaria sobre la conformidad de un sistema de IA. Por lo tanto, antes de poner a disposición sus sistemas de IA en la Unión, los proveedores establecidos

fuera de la Unión designarán, mediante mandato escrito, a un representante autorizado establecido en la Unión. Este representante autorizado desempeña un papel fundamental a la hora de garantizar la conformidad de los sistemas de IA de alto riesgo comercializados o puestos en servicio en la Unión por aquellos proveedores que no estén establecidos en la Unión y de actuar como su persona de contacto establecida en la Unión.

(56 bis)Habida cuenta de la naturaleza y la complejidad de la cadena de valor de los sistemas de IA y en consonancia con los principios del nuevo marco legislativo, es esencial garantizar la seguridad jurídica y facilitar el cumplimiento del presente Reglamento. Por lo tanto, es necesario aclarar el papel y las obligaciones específicas de los operadores pertinentes a lo largo de la cadena de valor, como los importadores y distribuidores que pueden contribuir al desarrollo de los sistemas de IA. En determinadas situaciones, esos operadores podrían actuar en más de una función al mismo tiempo y, por lo tanto, deberían cumplir acumulativamente todas las obligaciones pertinentes asociadas a esas funciones. Por ejemplo, un operador podría actuar como distribuidor e importador al mismo tiempo.

(57) Para garantizar la seguridad jurídica, es necesario aclarar que, en determinadas condiciones específicas, cualquier distribuidor, importador, implantador u otro tercero debe ser considerado proveedor de un sistema de IA de alto riesgo y, por tanto, asumir todas las obligaciones pertinentes. Este sería el caso si dicha parte pone su nombre o marca comercial en un sistema de IA de alto riesgo ya comercializado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo, o si dicha parte realiza una modificación sustancial en un sistema de IA de alto riesgo ya comercializado o puesto en servicio de forma que siga siendo un sistema de IA de alto riesgo de conformidad con el artículo 6 o si modifica la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido clasificado como de alto riesgo y que ya haya sido comercializado o puesto en servicio, de forma que el sistema de IA se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6. Estas disposiciones deben aplicarse sin perjuicio de disposiciones más específicas establecidas en determinadas normas sectoriales del nuevo marco legislativo con las que el presente Reglamento debe aplicarse conjuntamente. Por ejemplo, el artículo 16, apartado 2, del Reglamento 745/2017, que establece que determinados cambios no deben considerarse modificaciones de un producto que puedan afectar a su cumplimiento de los requisitos aplicables, debe seguir aplicándose a los sistemas de IA de alto riesgo que sean productos sanitarios en el sentido de dicho Reglamento.

(57 bis) Los sistemas de IA de propósito general pueden utilizarse como sistemas de IA de alto riesgo por sí mismos o ser componentes de otros sistemas de IA de alto riesgo. Por lo tanto, debido a su naturaleza particular y con el fin de garantizar un reparto equitativo de responsabilidades a lo largo de la cadena de valor de la IA, los proveedores de

dichos sistemas deben, con independencia de que puedan ser utilizados como sistemas de IA de alto riesgo como tales por otros proveedores o como componentes de sistemas de IA de alto riesgo y salvo disposición en contrario del presente Reglamento, cooperar estrechamente con los proveedores de los respectivos sistemas de IA de alto riesgo para permitirles cumplir las obligaciones pertinentes en virtud del presente Reglamento y con las autoridades competentes establecidas en virtud del presente Reglamento.

(57 ter) Cuando, en las condiciones establecidas en el presente Reglamento, el proveedor que inicialmente comercializó o puso en servicio el sistema de IA ya no deba ser considerado proveedor a efectos del presente Reglamento, y cuando dicho proveedor no haya excluido expresamente la transformación del sistema de IA en un sistema de IA de alto riesgo, el antiguo proveedor deberá, no obstante, cooperar estrechamente y facilitar la información necesaria y proporcionar el acceso técnico y demás asistencia que razonablemente quepa esperar y que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo.

(57 quater) Además, cuando un sistema de IA de alto riesgo que sea un componente de seguridad de un producto cubierto por una legislación sectorial del nuevo marco legislativo pertinente no se comercialice ni se ponga en servicio independientemente del producto, el fabricante del producto, tal como se define en la legislación del nuevo marco legislativo pertinente, deberá cumplir las obligaciones del proveedor establecidas en el presente Reglamento y, en particular, garantizar que el sistema de IA integrado en el producto final cumple los requisitos del presente Reglamento.

(57 quinquies) Dentro de la cadena de valor de la IA, múltiples partes suministran a menudo sistemas, herramientas y servicios de IA, pero también componentes o procesos que son incorporados por el proveedor al sistema de IA con diversos objetivos, incluido el entrenamiento del modelo, el reentrenamiento del modelo, la prueba y evaluación del modelo, la integración en programas informáticos u otros aspectos del desarrollo del modelo. Estas partes desempeñan un papel importante en la cadena de valor con respecto al proveedor del sistema de IA de alto riesgo en el que se integran sus sistemas, herramientas, servicios, componentes o procesos de IA, y deben proporcionar a este proveedor, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y demás asistencia necesarios basados en el estado de la técnica generalmente reconocido, a fin de que el proveedor pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento, sin comprometer sus propios derechos de propiedad intelectual o secretos comerciales.

(57 sexies) Los terceros que pongan a disposición del público herramientas, servicios, procesos o componentes de inteligencia artificial distintos de los modelos de inteligencia artificial de uso general no estarán obligados a cumplir los requisitos relativos a las responsabilidades a lo largo de la cadena de valor de la inteligencia artificial, en particular con respecto al proveedor.

que los haya utilizado o integrado, cuando esas herramientas, servicios, procesos o componentes de IA estén accesibles bajo una licencia libre y abierta. Debe animarse a los desarrolladores de herramientas, servicios, procesos o componentes de IA gratuitos y de código abierto distintos de los modelos de IA de uso general a que apliquen prácticas de documentación ampliamente adoptadas, como tarjetas de modelo y fichas de datos, como forma de acelerar el intercambio de información a lo largo de la cadena de valor de la IA, permitiendo la promoción de sistemas de IA fiables en la Unión.

(57 septies)La Comisión podría desarrollar y recomendar modelos de cláusulas contractuales voluntarias entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en sistemas de IA de alto riesgo, para facilitar la cooperación a lo largo de la cadena de valor. Al desarrollar modelos de condiciones contractuales voluntarias, la Comisión también debería tener en cuenta los posibles requisitos contractuales aplicables en sectores o casos empresariales específicos.

(58) Habida cuenta de la naturaleza de los sistemas de IA y de los riesgos para la seguridad y los derechos fundamentales que puede conllevar su utilización, incluida la necesidad de garantizar una supervisión adecuada del funcionamiento de un sistema de IA en un entorno real, conviene establecer responsabilidades específicas para los responsables del despliegue. En particular, los responsables del despliegue deben adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas de IA de alto riesgo de conformidad con las instrucciones de uso, y deben establecerse otras obligaciones en relación con la supervisión del funcionamiento de los sistemas de IA y con el mantenimiento de registros, según proceda. Además, los responsables del despliegue deben garantizar que las personas asignadas para aplicar las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento tengan la competencia necesaria, en particular un nivel adecuado de conocimientos de IA, formación y autoridad para desempeñar correctamente esas tareas. Estas obligaciones deben entenderse sin perjuicio de otras obligaciones de los responsables del despliegue en relación con los sistemas de IA de alto riesgo en virtud del Derecho de la Unión o nacional.

(58 ter) El presente Reglamento se entiende sin perjuicio de las obligaciones de los empresarios de informar o informar y consultar a los trabajadores o a sus representantes en virtud del Derecho y las prácticas de la Unión o nacionales, incluida la Directiva 2002/14/CE relativa a un marco general relativo a la información y a la consulta de los trabajadores, sobre las decisiones de poner en servicio o utilizar sistemas de IA. Sigue siendo necesario garantizar la información de los trabajadores y sus representantes sobre el despliegue previsto de sistemas de IA de alto riesgo en el lugar de trabajo en los casos en que no se cumplan las condiciones para dicha información o las obligaciones de información y consulta previstas en otros instrumentos jurídicos.

Además, dicho derecho de información es accesorio y necesario para el objetivo de protección de los derechos fundamentales que subyace en el presente Reglamento. Por lo tanto, un requisito de información a

a tal efecto debe establecerse en el presente Reglamento, sin que ello afecte a ninguno de los derechos existentes de los trabajadores.

(58 ter) Si bien los riesgos relacionados con los sistemas de IA pueden derivarse de la forma en que se diseñan dichos sistemas, los riesgos también pueden derivarse de la forma en que se utilizan dichos sistemas de IA. Por lo tanto, los implantadores de sistemas de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, complementando las obligaciones del proveedor al desarrollar el sistema de IA. Los encargados del despliegue son los más indicados para comprender cómo se utilizará concretamente el sistema de IA de alto riesgo y, por lo tanto, pueden identificar posibles riesgos significativos que no se hayan previsto en la fase de desarrollo, gracias a un conocimiento más preciso del contexto de uso y de las personas o grupos de personas que pueden verse afectados, incluidos los grupos vulnerables. Los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III también desempeñan un papel fundamental en la información a las personas físicas y deben, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, en su caso, informar a las personas físicas de que están sujetas al uso del sistema de IA de alto riesgo. Esta información deberá incluir la finalidad prevista y el tipo de decisiones que adopta. El implantador también debe informar a la persona física de su derecho a una explicación prevista en el presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo utilizados con fines policiales, esta obligación debe aplicarse de conformidad con el artículo 13 de la Directiva 2016/680.

(58 quinquies) Todo tratamiento de datos biométricos relacionado con el uso de sistemas de IA para la identificación biométrica con fines policiales debe cumplir lo dispuesto en el artículo 10 de la Directiva (UE) 2016/680, que permite dicho tratamiento únicamente cuando sea estrictamente necesario, con sujeción a las garantías adecuadas de los derechos y libertades del interesado, y cuando esté autorizado por el Derecho de la Unión o de los Estados miembros. Dicho uso, cuando esté autorizado, también debe respetar los principios establecidos en el artículo 4, apartado 1, de la Directiva (UE) 2016/680, incluida la licitud, la equidad y la transparencia, la limitación de la finalidad, la exactitud y la limitación del almacenamiento.

(58 sexies) Sin perjuicio del Derecho de la Unión aplicable, en particular el RGPD y la Directiva (UE) 2016/680 (Directiva sobre la aplicación de la ley), habida cuenta de la naturaleza intrusiva de los sistemas de identificación biométrica a distancia, el uso de sistemas de identificación biométrica a distancia estará sujeto a salvaguardias. Los sistemas de identificación biométrica a distancia deben utilizarse siempre de manera proporcionada, legítima y estrictamente necesaria, y, por lo tanto, de forma selectiva, en función de las personas que deban ser identificadas, la ubicación, el ámbito temporal y sobre la base de un conjunto de datos cerrado de secuencias de vídeo legalmente adquiridas. En cualquier caso, los sistemas de identificación biométrica a distancia no deben utilizarse en el marco de la aplicación de la ley para dar lugar a una identificación indiscriminada.

vigilancia. En cualquier caso, las condiciones para la identificación biométrica a distancia no deben servir de base para eludir las condiciones de la prohibición y las estrictas excepciones para la identificación biométrica a distancia en tiempo real.

(58 octies) Con el fin de garantizar eficazmente la protección de los derechos fundamentales, los implantadores 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 implanten determinados sistemas de IA de alto riesgo contemplados en el anexo III, como entidades bancarias o aseguradoras, deberán realizar una evaluación de impacto sobre los derechos fundamentales antes de ponerlo en funcionamiento. Los servicios importantes para las personas que son de carácter público también pueden ser prestados por entidades privadas. Los operadores privados que prestan estos servicios de carácter público están vinculados a tareas de interés público, como en el ámbito de la educación, la sanidad, los servicios sociales, la vivienda o la administración de justicia. El objetivo de la evaluación de impacto sobre los derechos fundamentales es que el implantador identifique los riesgos específicos para los derechos de las personas o grupos de personas que puedan verse afectados e identifique las medidas que deben adoptarse en caso de que se materialicen estos riesgos. La evaluación de impacto debe aplicarse al primer uso del sistema de IA de alto riesgo, y debe actualizarse cuando el implantador considere que ha cambiado alguno de los factores pertinentes. La evaluación de impacto debe identificar los procesos pertinentes del implantador en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista, y debe incluir una descripción del período de tiempo y la frecuencia en que se prevé utilizar el sistema, así como de las categorías específicas de personas físicas y grupos que puedan verse afectados en el contexto específico de utilización. La evaluación también debe incluir la identificación de riesgos específicos de daños que puedan afectar a los derechos fundamentales de estas personas o grupos. Al realizar esta evaluación, el responsable del despliegue debe tener en cuenta la información pertinente para una evaluación adecuada del impacto, incluida, entre otras, la información facilitada por el proveedor del sistema de IA de alto riesgo en las instrucciones de uso. A la luz de los riesgos identificados, los responsables del despliegue deben determinar las medidas que deben adoptarse en caso de que se materialicen estos riesgos, incluidas, por ejemplo, las disposiciones de gobernanza en ese contexto específico de uso, como las disposiciones para la supervisión humana con arreglo a las instrucciones de uso o los procedimientos de tramitación de reclamaciones y reparación, ya que podrían ser fundamentales para mitigar los riesgos para los derechos fundamentales en casos de uso concretos. Tras realizar esta evaluación de impacto, el implantador deberá notificarlo a la autoridad de vigilancia del mercado pertinente. Cuando proceda, para recopilar la información pertinente necesaria para realizar la evaluación de impacto, los implantadores de sistemas de IA de alto riesgo, en particular cuando los sistemas de IA se utilicen en el sector público, podrían implicar a las partes interesadas pertinentes, incluidos los representantes de los grupos de personas que puedan verse afectados por el sistema de IA.

sistema de IA, expertos independientes y organizaciones de la sociedad civil en la realización de dichas evaluaciones de impacto y en el diseño de las medidas a adoptar en caso de materialización de los riesgos. La Oficina de IA debería elaborar un modelo de cuestionario para facilitar el cumplimiento y reducir la carga administrativa de los responsables de la implantación.

(60 bis) La noción de modelos de IA de propósito general debe definirse claramente y diferenciarse de la noción de sistemas de IA para permitir la seguridad jurídica. La definición debe basarse en las características funcionales clave de un modelo de IA de propósito general, en particular la generalidad y la capacidad de realizar de forma competente una amplia gama de tareas distintas. Estos modelos suelen entrenarse con grandes cantidades de datos, a través de diversos métodos, como el aprendizaje autosupervisado, no supervisado o por refuerzo. Los modelos de IA de propósito general pueden comercializarse de diversas formas, como a través de bibliotecas, interfaces de programación de aplicaciones (API), como descarga directa o como copia física. Estos modelos pueden modificarse o perfeccionarse para crear otros nuevos. Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen sistemas de IA por sí solos. Los modelos de IA requieren la adición de otros componentes, como por ejemplo una interfaz de usuario, para convertirse en sistemas de IA. Los modelos de IA suelen integrarse en los sistemas de IA y formar parte de ellos. El presente Reglamento establece normas específicas para los modelos de IA de propósito general y para los modelos de IA de propósito general que plantean riesgos sistémicos, que deben aplicarse también cuando estos modelos se integran o forman parte de un sistema de IA. Debe entenderse que las obligaciones para los proveedores de modelos de IA de propósito general deben aplicarse una vez que los modelos de IA de propósito general se comercializan. Cuando el proveedor de un modelo de IA de propósito general integra un modelo propio en su propio sistema de IA que se comercializa o se pone en servicio, debe considerarse que dicho modelo se comercializa y, por lo tanto, deben seguir aplicándose las obligaciones previstas en el presente Reglamento para los modelos, además de las aplicables a los sistemas de IA. En cualquier caso, las obligaciones previstas para los modelos no deben aplicarse cuando un modelo propio se utilice para procesos puramente internos que no sean esenciales para proporcionar un producto o un servicio a terceros y no se vean afectados los derechos de las personas físicas. Teniendo en cuenta sus posibles efectos significativamente negativos, los modelos de IA de propósito general con riesgo sistémico deben estar siempre sujetos a las obligaciones pertinentes en virtud del presente Reglamento. La definición no debe abarcar los modelos de IA utilizados antes de su comercialización con el único fin de realizar actividades de investigación, desarrollo y creación de prototipos. Ello se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando, tras dichas actividades, se comercialice un modelo.

(60b) Mientras que la generalidad de un modelo podría, entre otros criterios, determinarse también por un número de parámetros, debería considerarse que los modelos con al menos mil millones de parámetros y entrenados con una gran cantidad de datos utilizando la autosupervisión a escala muestran una generalidad significativa y realizan de forma competente una amplia gama de tareas distintivas.

(60c)Los grandes modelos generativos de IA son un ejemplo típico de modelo de IA de propósito general, dado que permiten la generación flexible de contenidos (por ejemplo, en forma de texto, audio, imágenes o vídeo) que pueden acomodarse fácilmente a una amplia gama de tareas distintivas.

(60 quinquies) Cuando un modelo de IA de propósito general se integra en un sistema de IA o forma parte de él, este sistema debe considerarse un sistema de IA de propósito general cuando, debido a esta integración, este sistema tenga la capacidad de servir para diversos fines. Un sistema de IA de propósito general puede utilizarse directamente o puede integrarse en otros sistemas de IA.

(60 sexies) Los proveedores de modelos de IA de propósito general tienen un papel y una responsabilidad particulares en la cadena de valor de la IA, ya que los modelos que proporcionan pueden constituir la base de una serie de sistemas posteriores, a menudo proporcionados por proveedores posteriores que necesitan una buena comprensión de los modelos y sus capacidades, tanto para permitir la integración de dichos modelos en sus productos como para cumplir sus obligaciones en virtud de esta u otras normativas. Por lo tanto, deben preverse medidas de transparencia proporcionadas, incluida la elaboración y actualización de la documentación, y el suministro de información sobre el modelo de IA de propósito general para su uso por parte de los proveedores intermedios. El proveedor del modelo de IA de propósito general deberá elaborar y mantener al día la documentación técnica con el fin de ponerla a disposición de la Oficina de IA y de las autoridades nacionales competentes que la soliciten. El conjunto mínimo de elementos contenidos en dicha documentación debe esbozarse, respectivamente, en el Anexo (IXb) y en el Anexo (IXa). La Comisión debe estar facultada para modificar los anexos mediante actos delegados en función de la evolución tecnológica.

(60i) Los programas informáticos y los datos, incluidos los modelos, liberados bajo una licencia libre y de código abierto que permita compartirlos abiertamente y en la que los usuarios puedan acceder libremente a ellos , utilizarlos, modificarlos y redistribuirlos, o a versiones modificadas de los mismos, pueden contribuir a la investigación y la innovación en el mercado y ofrecer importantes oportunidades de crecimiento para la economía de la Unión.

Debe considerarse que los modelos de IA de propósito general publicados bajo licencias libres y de código abierto garantizan altos niveles de transparencia y apertura si sus parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo se ponen a disposición del público. La licencia debe considerarse libre y abierta.

fuente también cuando permite a los usuarios ejecutar, copiar, distribuir, estudiar, modificar y mejorar programas y datos informáticos, incluidos los modelos, con la condición de que se acredite al proveedor original del modelo y se respeten unas condiciones de distribución idénticas o comparables.

(60i+1) Los componentes de IA libres y de código abierto abarcan el software y los datos, incluidos los modelos y los modelos de IA de propósito general, las herramientas, los servicios o los procesos de un sistema de IA. Los componentes de IA libres y de código abierto pueden proporcionarse a través de diferentes canales, incluido su desarrollo en repositorios abiertos. A efectos del presente Reglamento, los componentes de IA que se faciliten a cambio de un precio o se moneticen de otro modo, incluso mediante la prestación de asistencia técnica u otros servicios, incluso a través de una plataforma de software, relacionados con el componente de IA, o el uso de datos personales por motivos distintos de los exclusivamente destinados a mejorar la seguridad, compatibilidad o interoperabilidad del software, con la excepción de las transacciones entre microempresas, no deben beneficiarse de las excepciones previstas para los componentes de IA gratuitos y de fuente abierta. El hecho de poner a disposición componentes de IA a través de repositorios abiertos no debe constituir, en sí mismo, una monetización.

(60 septies) Los proveedores de modelos de IA de propósito general que se publiquen con una licencia libre y de código abierto y cuyos parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público deben estar sujetos a excepciones por lo que respecta a los requisitos de transparencia impuestos a los modelos de IA de propósito general, a menos que pueda considerarse que presentan un riesgo sistémico, en cuyo caso la circunstancia de que el modelo sea transparente y vaya acompañado de una licencia de código abierto no debe considerarse razón suficiente para excluir el cumplimiento de las obligaciones previstas en el presente Reglamento. En cualquier caso, dado que la publicación de modelos de IA de propósito general bajo licencia gratuita y de código abierto no revela necesariamente información sustancial sobre el conjunto de datos utilizado para el entrenamiento o el ajuste del modelo y sobre cómo se ha garantizado el respeto de la legislación sobre derechos de autor, la excepción prevista para los modelos de IA de propósito general del cumplimiento de los requisitos relacionados con la transparencia no debe afectar a la obligación de elaborar un resumen sobre el contenido utilizado para el entrenamiento del modelo y la obligación de establecer una política para respetar la legislación de la Unión sobre derechos de autor, en particular para identificar y respetar las reservas de derechos expresadas de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790.

(60i)Los modelos de propósito general, en particular los grandes modelos generativos, capaces de generar texto, imágenes y otros contenidos, presentan oportunidades únicas de innovación, pero también retos para los artistas, autores y otros creadores y la forma en que se crean, distribuyen, utilizan y consumen sus contenidos creativos. El desarrollo y entrenamiento de estos modelos requiere el acceso a grandes cantidades de texto, imágenes, vídeos y otros datos. Las técnicas de minería de textos y datos pueden ser

utilizados ampliamente en este contexto para la recuperación y el análisis de dichos contenidos, que pueden estar protegidos por derechos de autor y derechos afines. Cualquier uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos en cuestión, a menos que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor. La Directiva (UE) 2019/790 introdujo excepciones y limitaciones que permiten reproducciones y extracciones de obras u otras materias, con fines de minería de textos y datos, en determinadas condiciones. En virtud de estas normas, los titulares de derechos pueden optar por reservar sus derechos sobre sus obras u otras materias para impedir la extracción de textos y datos, a menos que se haga con fines de investigación científica. Cuando los derechos de exclusión se hayan reservado expresamente de forma adecuada, los proveedores de modelos de IA de uso general deberán obtener una autorización de los titulares de los derechos si desean llevar a cabo minería de textos y datos sobre dichas obras.

(60 undecies) Los proveedores que comercialicen modelos de IA de propósito general en el mercado de la UE deben garantizar el cumplimiento de las obligaciones pertinentes del presente Reglamento. Para ello, los proveedores de modelos de IA de propósito general deben establecer una política de respeto del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para identificar y respetar las reservas de derechos expresadas por los titulares de derechos de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790. Cualquier proveedor que comercialice un modelo de IA de propósito general en el mercado de la UE debe cumplir con esta obligación, independientemente de la jurisdicción en la que tengan lugar los actos relevantes para los derechos de autor que sustentan la formación de estos modelos de IA de propósito general. Esto es necesario para garantizar la igualdad de condiciones entre los proveedores de modelos de IA de propósito general, donde ningún proveedor debería poder obtener una ventaja competitiva en el mercado de la UE aplicando normas de derechos de autor inferiores a las previstas en la Unión.

(60 duodecies) Con el fin de aumentar la transparencia sobre los datos que se utilizan en el preentrenamiento y el entrenamiento de los modelos de IA de propósito general, incluidos los textos y datos protegidos por la legislación sobre derechos de autor, es adecuado que los proveedores de dichos modelos elaboren y pongan a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de propósito general. Si bien debe tenerse debidamente en cuenta la necesidad de proteger los secretos comerciales y la información empresarial confidencial, este resumen debe tener un alcance general, en lugar de ser técnicamente detallado, para facilitar a las partes con intereses legítimos, incluidos los titulares de derechos de autor, el ejercicio y la aplicación de sus derechos con arreglo al Derecho de la Unión, por ejemplo enumerando las principales colecciones o conjuntos de datos que se utilizaron para entrenar el modelo, como grandes bases de datos privadas o públicas o archivos de datos, y proporcionando una explicación narrativa sobre otras fuentes de datos utilizadas. Conviene que la Oficina de AI facilite una plantilla para el resumen,

que debe ser simple, eficaz y permitir al proveedor proporcionar el resumen requerido en forma narrativa.

(60 quinquies)Por lo que respecta a las obligaciones impuestas a los proveedores de modelos de IA de propósito general de establecer una política de respeto de la legislación de la Unión en materia de derechos de autor y poner a disposición del público un resumen del contenido utilizado para la formación, la Oficina de IA debe supervisar si el proveedor ha cumplido dichas obligaciones sin verificar ni proceder a una evaluación obra por obra de los datos de formación en términos de cumplimiento de los derechos de autor. El presente Reglamento no afecta a la aplicación de las normas sobre derechos de autor previstas en el Derecho de la Unión.

(60 octies) El cumplimiento de las obligaciones previstas para los proveedores de modelos de IA de propósito general debe ser proporcional al tipo de proveedor de modelos, excluyendo la necesidad de cumplimiento para las personas que desarrollen o utilicen modelos con fines no profesionales o de investigación científica, a las que, no obstante, debe animarse a cumplir voluntariamente estos requisitos. Sin perjuicio de la legislación de la Unión sobre derechos de autor, el cumplimiento de estas obligaciones debe tener debidamente en cuenta el tamaño del proveedor y permitir formas simplificadas de cumplimiento para las PYME, incluidas las empresas de nueva creación, que no deben representar un coste excesivo ni desalentar el uso de tales modelos. En caso de modificación o ajuste de un modelo, las obligaciones de los proveedores deben limitarse a dicha modificación o ajuste, por ejemplo complementando la documentación técnica ya existente con información sobre las modificaciones, incluidas las nuevas fuentes de datos de formación, como medio para cumplir las obligaciones de la cadena de valor previstas en el presente Reglamento.

(60m)Los modelos de IA de propósito general podrían plantear riesgos sistémicos que incluyen, entre otros, cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, interrupciones de sectores críticos y consecuencias graves para la salud y la seguridad públicas; cualquier efecto negativo real o razonablemente previsible en los procesos democráticos, la seguridad pública y económica; la difusión de contenidos ilegales, falsos o discriminatorios. Debe entenderse que los riesgos sistémicos aumentan con las capacidades y el alcance del modelo, pueden surgir a lo largo de todo el ciclo de vida del modelo y se ven influidos por las condiciones de uso indebido, la fiabilidad del modelo, la imparcialidad y la seguridad del modelo, el grado de autonomía del modelo, su acceso a herramientas, modalidades novedosas o combinadas, estrategias de liberación y distribución, el potencial para eliminar barreras de protección y otros factores. En particular, los enfoques internacionales han identificado hasta ahora la necesidad de dedicar atención a los riesgos derivados de un posible uso indebido intencionado o de cuestiones de control no intencionadas relacionadas con la alineación con la intención humana; los riesgos químicos, biológicos, radiológicos y nucleares, como las formas en que pueden reducirse las barreras de entrada, incluso para el desarrollo de armas, la adquisición de diseños o su uso; las ofensivas

las capacidades cibernéticas, como las formas en que puede permitirse el descubrimiento de vulnerabilidades, la explotación o el uso operativo; los efectos de la interacción y el uso de herramientas, incluida, por ejemplo, la capacidad de controlar sistemas físicos e interferir en infraestructuras críticas; los riesgos de que los modelos hagan copias de sí mismos o se "autorrepliquen" o entrenen a otros modelos; las formas en que los modelos pueden dar lugar a prejuicios y discriminaciones perjudiciales con riesgos para las personas, las comunidades o las sociedades; la facilitación de la desinformación o el perjuicio de la privacidad con amenazas para los valores democráticos y los derechos humanos; el riesgo de que un acontecimiento concreto pueda dar lugar a una reacción en cadena con efectos negativos considerables que podrían afectar hasta a toda una ciudad, toda una actividad de dominio o toda una comunidad.

(60n) Conviene establecer una metodología para la clasificación de los modelos de IA de propósito general como modelos de IA de propósito general con riesgos sistémicos. Dado que los riesgos sistémicos se derivan de capacidades particularmente elevadas, debe considerarse que un modelo de IA de propósito general presenta riesgos sistémicos si tiene capacidades de alto impacto, evaluadas sobre la base de herramientas técnicas y metodologías adecuadas, o un impacto significativo en el mercado interior debido a su alcance. Por capacidades de alto impacto en modelos de IA de propósito general se entienden capacidades que igualan o superan las capacidades registradas en los modelos de IA de propósito general más avanzados. La gama completa de capacidades de un modelo podría comprenderse mejor tras su lanzamiento al mercado o cuando los usuarios interactúen con el modelo. Según el estado de la técnica en el momento de la entrada en vigor del presente Reglamento, la cantidad acumulada de cálculo utilizada para el entrenamiento del modelo de IA de propósito general, medida en operaciones en coma flotante (FLOPs), es una de las aproximaciones pertinentes a las capacidades del modelo. La cantidad de cálculo utilizada para el entrenamiento acumula el cálculo utilizado en todas las actividades y métodos destinados a mejorar las capacidades del modelo antes de su despliegue, como el preentrenamiento, la generación de datos sintéticos y el ajuste fino. Por lo tanto, debe fijarse un umbral inicial de FLOPs que, si lo alcanza un modelo de IA de propósito general, lleve a presumir que se trata de un modelo de IA de propósito general con riesgos sistémicos. Este umbral debería ajustarse con el tiempo para reflejar los cambios tecnológicos e industriales, como las mejoras algorítmicas o el aumento de la eficiencia del hardware, y debería complementarse con puntos de referencia e indicadores de la capacidad del modelo. Para ello, la Oficina de Inteligencia Artificial debería colaborar con la comunidad científica, la industria, la sociedad civil y otros expertos. Los umbrales, así como las herramientas y los puntos de referencia para la evaluación de las capacidades de alto impacto, deberían ser sólidos predictores de la generalidad, sus capacidades y el riesgo sistémico asociado de los modelos de IA de propósito general, y podrían tener en cuenta la forma en que el modelo se comercializará o el número de usuarios a los que puede afectar. Para complementar este sistema, debería existir la posibilidad de

que la Comisión adopte decisiones individuales por las que se designe un modelo de IA de propósito general como modelo de IA de propósito general con riesgo sistémico si se constata que dicho modelo tiene capacidades o un impacto equivalentes a los captados por el umbral establecido. Esta decisión deberá adoptarse sobre la base de una evaluación global de los criterios establecidos en el anexo YY, como la calidad o el tamaño del conjunto de datos de entrenamiento, el número de empresas y usuarios finales, sus modalidades de entrada y salida, su grado de autonomía y escalabilidad, o las herramientas a las que tiene acceso. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de propósito general con riesgo sistémico, la Comisión deberá tener en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de propósito general presenta riesgos sistémicos.

(60 sexdecies) También es necesario aclarar un procedimiento para la clasificación de un modelo de IA de propósito general con riesgos sistémicos. Un modelo de IA de propósito general que alcance el umbral aplicable a las capacidades de alto impacto debe presumirse que es un modelo de IA de propósito general con riesgo sistémico. El proveedor deberá notificarlo a la Oficina de IA a más tardar dos semanas después de que se cumplan los requisitos o de que se tenga conocimiento de que un modelo de IA de propósito general cumplirá los requisitos que dan lugar a la presunción. Esto es especialmente relevante en relación con el umbral FLOP porque la formación de modelos de IA de propósito general requiere una planificación considerable que incluye la asignación por adelantado de recursos informáticos y, por lo tanto, los proveedores de modelos de IA de propósito general pueden saber si su modelo cumpliría el umbral antes de que finalice la formación. En el contexto de esta notificación, el proveedor debe poder demostrar que, debido a sus características específicas, un modelo de IA de propósito general no presenta excepcionalmente riesgos sistémicos y que, por tanto, no debe clasificarse como modelo de IA de propósito general con riesgos sistémicos. Esta información es valiosa para que la Oficina de IA pueda anticiparse a la comercialización de modelos de IA de propósito general con riesgos sistémicos y los proveedores puedan empezar a colaborar con la Oficina de IA en una fase temprana. Esto es especialmente importante en lo que respecta a los modelos de IA de propósito general que está previsto comercializar como código abierto, dado que, tras la comercialización del modelo como código abierto, puede resultar más difícil aplicar las medidas necesarias para garantizar el cumplimiento de las obligaciones previstas en el presente Reglamento.

(60p) Si la Comisión tiene conocimiento de que un modelo de IA de propósito general cumple los requisitos para ser clasificado como modelo de IA de propósito general con riesgo sistémico, lo que anteriormente no se sabía o de lo que el proveedor correspondiente no ha informado a la Comisión, ésta debe estar facultada para designarlo como tal. Un sistema de alertas cualificadas debe garantizar que la Oficina de IA sea informada por el panel científico de

modelos de IA de propósito general que posiblemente deberían clasificarse como modelos de IA de propósito general con riesgo sistémico, además de las actividades de supervisión de la Oficina de IA.

(60 octodecies) Los proveedores de modelos de IA de propósito general que presenten riesgos sistémicos deben estar sujetos, además de a las obligaciones previstas para los proveedores de modelos de IA de propósito general, a obligaciones destinadas a identificar y mitigar dichos riesgos y a garantizar un nivel adecuado de protección de la ciberseguridad, independientemente de si se proporciona como modelo independiente o integrado en un sistema o producto de IA. Para alcanzar estos objetivos, el Reglamento debe exigir a los proveedores que realicen las evaluaciones necesarias de los modelos, en particular antes de su primera comercialización, incluida la realización y documentación de pruebas adversariales de los modelos, también, según proceda, mediante pruebas internas o externas independientes. Además, los proveedores de modelos de IA de propósito general con riesgos sistémicos deben evaluar y mitigar continuamente los riesgos sistémicos, por ejemplo, estableciendo políticas de gestión de riesgos, como procesos de rendición de cuentas y gobernanza, aplicando un seguimiento posterior a la comercialización, adoptando medidas adecuadas a lo largo de todo el ciclo de vida del modelo y cooperando con los agentes pertinentes en toda la cadena de valor de la IA.

(60r) Los proveedores de modelos de IA de propósito general con riesgos sistémicos deben evaluar y mitigar los posibles riesgos sistémicos. Si, a pesar de los esfuerzos por identificar y prevenir los riesgos relacionados con un modelo de IA de propósito general que pueda presentar riesgos sistémicos, el desarrollo o uso del modelo provoca un incidente grave, el proveedor del modelo de IA de propósito general debe, sin demora indebida, hacer un seguimiento del incidente y comunicar toda la información pertinente y las posibles medidas correctoras a la Comisión y a las autoridades nacionales competentes. Además, los proveedores deben garantizar un nivel adecuado de protección de la ciberseguridad para el modelo y su infraestructura física, si procede, a lo largo de todo el ciclo de vida del modelo. La protección de la 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 liberaciones 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, algoritmos, servidores y conjuntos de datos de los modelos, por ejemplo mediante medidas de seguridad operativa para la seguridad de la información, políticas específicas de ciberseguridad, soluciones técnicas adecuadas y establecidas, y controles de acceso cibernético y físico, adecuados a las circunstancias pertinentes y a los riesgos implicados.

(60s) La Oficina de IA debería fomentar y facilitar la elaboración, revisión y adaptación de Códigos de Prácticas, teniendo en cuenta los enfoques internacionales. Podría invitarse a participar a todos los proveedores de modelos de IA de uso general. Para garantizar que los Códigos de buenas prácticas reflejen el estado de la técnica y tengan debidamente en cuenta un conjunto diverso de perspectivas, la Oficina de AI

La Oficina debería colaborar con las autoridades nacionales competentes y podría, en su caso, consultar a las organizaciones de la sociedad civil y a otras partes interesadas y expertos pertinentes, incluido el Grupo Científico, para la elaboración de los Códigos. Los Códigos de buenas prácticas deben cubrir las obligaciones de los proveedores de modelos de IA de propósito general y de modelos de propósito general que presenten riesgos sistémicos. Además, por lo que se refiere a los riesgos sistémicos, los Códigos de buenas prácticas deben contribuir a establecer una taxonomía de riesgos del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluidas sus fuentes. Los Códigos de buenas prácticas también deberían centrarse en medidas específicas de evaluación y mitigación de riesgos.

(60 unvicies) Los Códigos de buenas prácticas deben representar una herramienta central para el correcto cumplimiento de las obligaciones previstas en el presente Reglamento para los proveedores de modelos de IA de propósito general. Los proveedores deben poder basarse en los Códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. Mediante actos de ejecución, la Comisión podrá decidir aprobar un código de buenas prácticas y darle una validez general en la Unión o, alternativamente, establecer normas comunes para la aplicación de las obligaciones pertinentes, si, en el momento en que el Reglamento sea aplicable, no se puede ultimar un código de buenas prácticas o la Oficina de IA no lo considera adecuado. Una vez publicada una norma armonizada y evaluada como adecuada para cubrir las obligaciones pertinentes por la Oficina de IA, el cumplimiento de una norma armonizada europea debería otorgar a los proveedores la presunción de conformidad. Además, los proveedores de modelos de IA de propósito general deben poder demostrar el cumplimiento utilizando medios alternativos adecuados, si no se dispone de códigos de prácticas o normas armonizadas, o si deciden no basarse en ellos.

(60 duovicies) El presente Reglamento regula los sistemas y modelos de IA imponiendo determinados requisitos y obligaciones a los agentes del mercado pertinentes que los comercialicen, pongan en servicio o utilicen en la Unión, complementando así las obligaciones para los proveedores de servicios de intermediación que integren dichos sistemas o modelos en sus servicios regulados por el Reglamento (UE) 2022/2065. En la medida en que tales sistemas o modelos estén integrados en plataformas en línea muy grandes o motores de búsqueda en línea muy grandes designados, estarán sujetos al marco de gestión de riesgos previsto en el Reglamento (UE) 2022/2065.

En consecuencia, debe presumirse que se cumplen las obligaciones correspondientes de la Ley de IA, a menos que surjan y se identifiquen en dichos modelos riesgos sistémicos significativos no cubiertos por el Reglamento (UE) 2022/2065. En este marco, los proveedores de plataformas en línea muy grandes y de motores de búsqueda muy grandes están obligados a evaluar los posibles riesgos sistémicos derivados del diseño, funcionamiento y uso de sus servicios, incluido el modo en que el diseño de los sistemas algorítmicos utilizados en el servicio puede contribuir a tales riesgos, así como a

riesgos sistémicos derivados de posibles usos indebidos. Dichos proveedores también están obligados a adoptar las medidas paliativas adecuadas en cumplimiento de los derechos fundamentales.

(60 bis bis) Teniendo en cuenta el rápido ritmo de la innovación y la evolución tecnológica de los servicios digitales en el ámbito de aplicación de diferentes instrumentos del Derecho de la Unión, en particular teniendo en cuenta el uso y la percepción de sus destinatarios, los sistemas de IA sujetos al presente Reglamento pueden prestarse como servicios de intermediación o partes de los mismos en el sentido del Reglamento (UE) 2022/2065, que debe interpretarse de manera tecnológicamente neutra. Por ejemplo, los sistemas de IA pueden utilizarse para proporcionar motores de búsqueda en línea, en particular, en la medida en que un sistema de IA como un chatbot en línea realiza búsquedas de, en principio, todos los sitios web, a continuación incorpora los resultados a sus conocimientos existentes y utiliza los conocimientos actualizados para generar un único resultado que combina diferentes fuentes de información.

(60v) Además, las obligaciones impuestas a los proveedores y a los implantadores de determinados sistemas de IA en el presente Reglamento para permitir la detección y divulgación de que los resultados de dichos sistemas se han generado o manipulado artificialmente son especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular a las obligaciones de los proveedores de plataformas en línea muy grandes o de motores de búsqueda en línea muy grandes de identificar y mitigar los riesgos sistémicos que puedan derivarse de la difusión de contenidos generados o manipulados artificialmente, en particular el riesgo de los efectos negativos reales o previsibles en los procesos democráticos, el discurso cívico y los procesos electorales, incluso a través de la desinformación.

---

(61) La normalización debe desempeñar un papel clave para ofrecer soluciones técnicas a los proveedores que garanticen el cumplimiento del presente Reglamento, en consonancia con el estado de la técnica, a fin de promover la innovación, así como la competitividad y el crecimiento en el mercado único. El cumplimiento de las normas armonizadas definidas en el Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo[25] , de las que normalmente se espera que reflejen el estado de la técnica, debe ser un medio para que los proveedores demuestren la conformidad con los requisitos del presente Reglamento. Por consiguiente, debe fomentarse una representación equilibrada de los intereses en la que participen todas las partes interesadas pertinentes en la elaboración de las normas, en particular las PYME, las organizaciones de consumidores y las partes interesadas medioambientales y sociales, de conformidad con los artículos 5 y 6 del Reglamento 1025/2012. Para facilitar el cumplimiento, las solicitudes de normalización deben ser

[25] Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea y por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y se derogan la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

emitida por la Comisión sin demoras indebidas. Al preparar la solicitud de normalización, la Comisión debe consultar al Foro consultivo de la IA y al Consejo para recabar los conocimientos técnicos pertinentes. No obstante, a falta de referencias pertinentes a normas armonizadas, la Comisión debe poder establecer, mediante actos de ejecución y previa consulta al Foro consultivo de la IA, especificaciones comunes para determinados requisitos con arreglo al presente Reglamento. La especificación común debe ser una solución de emergencia excepcional para facilitar la obligación del proveedor de cumplir los requisitos del presente Reglamento, cuando la solicitud de normalización no haya sido aceptada por ninguna de las organizaciones europeas de normalización, o cuando las normas armonizadas pertinentes no aborden suficientemente las preocupaciones en materia de derechos fundamentales, o cuando las normas armonizadas no se ajusten a la solicitud, o cuando se produzcan retrasos en la adopción de una norma armonizada adecuada. Si dicho retraso en la adopción de una norma armonizada se debe a la complejidad técnica de la norma en cuestión, la Comisión deberá tenerlo en cuenta antes de contemplar el establecimiento de especificaciones comunes. A la hora de desarrollar especificaciones comunes, se anima a la Comisión a cooperar con socios internacionales y organismos internacionales de normalización.

(61 bis) Conviene que, sin perjuicio del uso de normas armonizadas y especificaciones comunes, se presuma que los proveedores de sistemas de IA de alto riesgo que hayan sido formados y probados con datos que reflejen el entorno geográfico, conductual, contextual o funcional específico en el que se pretende utilizar el sistema de IA cumplen la medida respectiva prevista en el marco del requisito sobre gobernanza de datos establecido en el presente Reglamento. Sin perjuicio de los requisitos relacionados con la solidez y la precisión establecidos en el presente Reglamento, en consonancia con el artículo 54, apartado 3, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, debe presumirse que los sistemas de IA de alto riesgo que hayan sido certificados o para los que se haya expedido una declaración de conformidad en el marco de un régimen de ciberseguridad con arreglo a dicho Reglamento y cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea cumplen el requisito de ciberseguridad del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad o partes de los mismos cubran el requisito de ciberseguridad del presente Reglamento Esto se mantiene sin perjuicio del carácter voluntario de dicho régimen de ciberseguridad.

(62) Para garantizar un alto nivel de fiabilidad de los sistemas de IA de alto riesgo, dichos sistemas deben someterse a una evaluación de conformidad antes de su comercialización o puesta en servicio.

Conviene que, a fin de reducir al mínimo la carga para los operadores y evitar cualquier posible duplicación, en el caso de los sistemas de IA de alto riesgo relacionados con productos que están cubiertos por la legislación de armonización de la Unión existente siguiendo el enfoque del nuevo marco legislativo, el cumplimiento de dichos sistemas de IA con los requisitos del presente Reglamento se evalúe como parte de la evaluación de la conformidad ya prevista en virtud de dicha legislación. Así pues, la aplicabilidad de los requisitos del presente Reglamento no debe afectar a la lógica específica, la metodología o la estructura general de la evaluación de la conformidad con arreglo a la legislación específica pertinente del nuevo marco legislativo.

(63) Dada la complejidad de los sistemas de IA de alto riesgo y los riesgos que llevan asociados, es importante desarrollar un sistema adecuado de procedimiento de evaluación de la conformidad para los sistemas de IA de alto riesgo en el que participen organismos notificados, la denominada evaluación de la conformidad por terceros. No obstante, habida cuenta de la experiencia actual de los certificadores profesionales previos a la comercialización en el ámbito de la seguridad de los productos y de la diferente naturaleza de los riesgos implicados, conviene limitar, al menos en una fase inicial de aplicación del presente Reglamento, el ámbito de aplicación de la evaluación de la conformidad por terceros para los sistemas de IA de alto riesgo distintos de los relacionados con los productos. Por consiguiente, la evaluación de la conformidad de dichos sistemas debe realizarla, como norma general, el proveedor bajo su propia responsabilidad, con la única excepción de los sistemas de IA destinados a utilizarse para la biometría.

(64) Con el fin de llevar a cabo evaluaciones de la conformidad por terceros cuando así se requiera, los organismos notificados deben ser notificados con arreglo al presente Reglamento por las autoridades nacionales competentes, siempre que cumplan una serie de requisitos, en particular en materia de independencia, competencia, ausencia de conflictos de intereses y requisitos de ciberseguridad adecuados. Las autoridades nacionales competentes deben enviar la notificación de dichos organismos a la Comisión y a los demás Estados miembros por medio de la herramienta de notificación electrónica desarrollada y gestionada por la Comisión con arreglo al artículo R23 de la Decisión 768/2008.

(65 bis) En consonancia con los compromisos de la Unión en virtud del Acuerdo sobre Obstáculos Técnicos al Comercio de la Organización Mundial del Comercio, es adecuado facilitar el reconocimiento mutuo de los resultados de la evaluación de la conformidad producidos por organismos de evaluación de la conformidad competentes, independientemente del territorio en el que estén establecidos, siempre que dichos organismos de evaluación de la conformidad establecidos con arreglo a la legislación de un tercer país cumplan los requisitos aplicables del Reglamento y la Unión haya celebrado un acuerdo en ese sentido. En este contexto, la Comisión debe explorar activamente posibles instrumentos internacionales a tal efecto y, en particular, perseguir la celebración de acuerdos de reconocimiento mutuo con terceros países.

En consonancia con la noción comúnmente establecida de modificación sustancial de los productos regulados por la legislación de armonización de la Unión, conviene que, siempre que se produzca un cambio que pueda afectar a la conformidad de un sistema de IA de alto riesgo con el presente Reglamento (por ejemplo, cambio del sistema operativo o de la arquitectura del software), o cuando cambie la finalidad prevista del sistema, dicho sistema de IA debe considerarse un nuevo sistema de IA que debe someterse a una nueva evaluación de la conformidad. No obstante, los cambios que se produzcan en el algoritmo y el rendimiento de los sistemas de IA que sigan "aprendiendo" después de su comercialización o puesta en servicio (es decir, que adapten automáticamente la forma en que se llevan a cabo las funciones) no deben constituir una modificación sustancial, siempre que dichos cambios hayan sido determinados previamente por el proveedor y evaluados en el momento de la evaluación de la conformidad.

(65) Los sistemas de IA de alto riesgo deben llevar el marcado CE para indicar su conformidad con el presente Reglamento, de modo que puedan circular libremente en el mercado interior. En el caso de los sistemas de IA de alto riesgo integrados en un producto, debe colocarse un marcado CE físico, que puede complementarse con un marcado CE digital. En el caso de los sistemas de IA de alto riesgo suministrados únicamente de forma digital, debe utilizarse un marcado CE digital. Los Estados miembros no deben crear obstáculos injustificados a la comercialización o puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

(66) En determinadas condiciones, la rápida disponibilidad de tecnologías innovadoras puede ser crucial para la salud y la seguridad de las personas, la protección del medio ambiente y el cambio climático y para la sociedad en su conjunto. Así pues, conviene que, por razones excepcionales de seguridad pública o de protección de la vida y la salud de las personas físicas, de protección del medio ambiente y de protección de activos industriales e infraestructurales clave, las autoridades de vigilancia del mercado puedan autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA que no hayan sido objeto de una evaluación de conformidad. En situaciones debidamente justificadas según lo dispuesto en este reglamento, las autoridades policiales o las autoridades de protección civil podrán poner en servicio un sistema de IA específico de alto riesgo sin la autorización de la autoridad de vigilancia del mercado, siempre que dicha autorización se solicite durante o después del uso sin demora indebida.

(67) Para facilitar el trabajo de la Comisión y de los Estados miembros en el ámbito de la inteligencia artificial, así como para aumentar la transparencia de cara al público, los proveedores de sistemas de inteligencia artificial de alto riesgo distintos de los relacionados con productos incluidos en el ámbito de aplicación de la legislación de armonización de la Unión vigente, así como los proveedores que consideren que un sistema de inteligencia artificial mencionado en el anexo III no es de alto riesgo por excepción, deben estar obligados a registrarse ellos mismos y a registrar la información sobre su sistema de inteligencia artificial en una base de datos de la UE, que será

establecida y gestionada por la Comisión. Antes de utilizar un sistema de IA de alto riesgo enumerado en el anexo III, los implantadores de sistemas de IA de alto riesgo que sean autoridades, agencias u organismos públicos deberán registrarse en dicha base de datos y seleccionar el sistema que prevén utilizar. Los demás implantadores podrán hacerlo voluntariamente. Esta sección de la base de datos debe ser de acceso público y gratuito, la información debe ser fácilmente navegable, comprensible y legible por máquina. La base de datos también debe ser fácil de usar, por ejemplo, proporcionando funciones de búsqueda, incluso mediante palabras clave, que permitan al público en general encontrar información pertinente incluida en el anexo VIII y sobre los ámbitos de riesgo del anexo III a los que corresponden los sistemas de IA de alto riesgo. Cualquier modificación sustancial de los sistemas de IA de alto riesgo también deberá registrarse en la base de datos de la UE. En el caso de los sistemas de IA de alto riesgo en el ámbito de la aplicación de la ley, la migración, el asilo y la gestión del control fronterizo, las obligaciones de registro deberán cumplirse en una sección segura no pública de la base de datos. El acceso a la sección no pública segura debe limitarse estrictamente a la Comisión y a las autoridades de vigilancia del mercado en lo que respecta a su sección nacional de la base de datos. Los sistemas de IA de alto riesgo en el ámbito de las infraestructuras críticas sólo deben registrarse a nivel nacional. La Comisión debe ser el controlador de la base de datos de la UE, de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[26] . Para garantizar la plena funcionalidad de la base de datos, cuando se despliegue, el procedimiento para establecer la base de datos debe incluir la elaboración de especificaciones funcionales por parte de la Comisión y un informe de auditoría independiente. La Comisión debería tener en cuenta los riesgos relacionados con la ciberseguridad y la peligrosidad a la hora de llevar a cabo sus tareas como responsable del tratamiento de datos en la base de datos de la UE. Para maximizar la disponibilidad y el uso de la base de datos por parte del público, la base de datos, incluida la información disponible a través de ella, debe cumplir los requisitos establecidos en la Directiva 2019/882.

(68) Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden plantear riesgos específicos de suplantación de identidad o engaño, con independencia de que se califiquen o no de alto riesgo. En determinadas circunstancias, el uso de estos sistemas debería, por tanto, estar sujeto a obligaciones específicas de transparencia sin perjuicio de los requisitos y obligaciones para los sistemas de IA de alto riesgo y sujeto a excepciones específicas para tener en cuenta la necesidad especial de las fuerzas y cuerpos de seguridad. En particular, deberá notificarse a las personas físicas que están interactuando con un sistema de IA, a menos que ello resulte obvio desde el punto de vista de una persona física razonablemente bien informada, observadora y perspicaz teniendo en cuenta

[26] 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) (DO L 119 de 4.5.2016, p. 1).

las circunstancias y el contexto de uso. Al aplicar dicha obligación, deben tenerse en cuenta las características de las personas pertenecientes a grupos vulnerables debido a su edad o discapacidad, en la medida en que el sistema de IA esté destinado a interactuar también con dichos grupos. Además, las personas físicas deben ser notificadas cuando estén expuestas a sistemas que, mediante el tratamiento de sus datos biométricos, puedan identificar o inferir las emociones o intenciones de dichas personas o asignarlas a categorías específicas. Dichas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos personales, el origen étnico, las preferencias personales y los intereses. Dicha información y notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad.

(70 bis) Diversos sistemas de IA pueden generar grandes cantidades de contenidos sintéticos que resultan cada vez más difíciles de distinguir para los seres humanos de los contenidos auténticos y generados por ellos. La amplia disponibilidad y las crecientes capacidades de esos sistemas tienen un impacto significativo en la integridad y la confianza en el ecosistema de la información, planteando nuevos riesgos de desinformación y manipulación a escala, fraude, suplantación de identidad y engaño al consumidor. A la luz de esas repercusiones, del rápido ritmo tecnológico y de la necesidad de nuevos métodos y técnicas para rastrear el origen de la información, conviene exigir a los proveedores de esos sistemas que incorporen soluciones técnicas que permitan el marcado en un formato legible por máquina y la detección de que el resultado ha sido generado o manipulado por un sistema de IA y no por un ser humano. Dichas técnicas y métodos deben ser suficientemente fiables, interoperables, eficaces y sólidos en la medida en que sea técnicamente viable, teniendo en cuenta las técnicas disponibles o una combinación de dichas técnicas, como marcas de agua, identificaciones de metadatos, métodos criptográficos para demostrar la procedencia y autenticidad de los contenidos, métodos de registro, huellas dactilares u otras técnicas, según proceda. Al aplicar esta obligación, los proveedores también deben tener en cuenta las especificidades y las limitaciones de los diferentes tipos de contenidos y los avances tecnológicos y de mercado pertinentes en este ámbito, tal como se refleja en el estado de la técnica generalmente reconocido. Dichas técnicas y métodos pueden aplicarse a nivel del sistema o a nivel del modelo, incluidos los modelos de IA de propósito general que generan contenidos, facilitando así el cumplimiento de esta obligación por parte del proveedor posterior del sistema de IA. Para mantener la proporcionalidad, conviene prever que esta obligación de marcado no cubra los sistemas de IA que desempeñen principalmente una función de asistencia para la edición estándar o los sistemas de IA que no alteren sustancialmente los datos de entrada proporcionados por el usuario o la semántica de los mismos.

(70b)Además de las soluciones técnicas empleadas por los proveedores del sistema, los implantadores , que utilizan un sistema de IA para generar o manipular contenidos de imagen, audio o vídeo que apreciablemente

El cumplimiento de esta obligación de transparencia no debe interpretarse en el sentido de que el uso del sistema o de sus resultados impida el derecho a la libertad de expresión y el derecho a la libertad de las artes y las ciencias garantizados en la Carta de los Derechos Fundamentales de la UE, en particular cuando el contenido forme parte de una obra o programa evidentemente creativo, satírico, artístico o de ficción, siempre que se garanticen adecuadamente los derechos y libertades de terceros. En esos casos, la obligación de transparencia para las falsificaciones profundas establecida en el presente Reglamento se limita a la divulgación de la existencia de esos contenidos generados o manipulados de una manera adecuada que no obstaculice la exhibición o el disfrute de la obra, incluida su explotación y uso normales, manteniendo al mismo tiempo la utilidad y calidad de la obra. Además, también procede prever una obligación de divulgación similar en relación con el texto generado o manipulado por IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado por IA haya sido sometido a un proceso de revisión humana o control editorial y una persona física o jurídica ostente la responsabilidad editorial de la publicación del contenido.

(70 quater) Para garantizar una aplicación coherente, conviene facultar a la Comisión para que adopte actos de ejecución sobre la aplicación de las disposiciones relativas al etiquetado y la detección de contenidos generados artificialmente o manipulados. Sin perjuicio del carácter obligatorio y de la plena aplicabilidad de estas obligaciones, la Comisión también podrá fomentar y facilitar la elaboración de códigos de prácticas a escala de la Unión para facilitar la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados artificialmente, incluido el apoyo a disposiciones prácticas para hacer accesibles, según proceda, los mecanismos de detección y facilitar la cooperación con otros agentes de la cadena de valor, difundir contenidos o comprobar su autenticidad y procedencia para que el público pueda distinguir efectivamente los contenidos generados por IA.

(70 quinquies) Las obligaciones impuestas en el presente Reglamento a los proveedores e implantadores de determinados sistemas de IA para permitir la detección y divulgación de que los resultados de dichos sistemas se han generado o manipulado artificialmente son especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular en lo que respecta a las obligaciones de los proveedores de plataformas en línea muy grandes o motores de búsqueda en línea muy grandes de identificar y mitigar los riesgos sistémicos que puedan derivarse de la difusión de contenidos que hayan sido

generados artificialmente o manipulados, en particular el riesgo de los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, incluso a través de la desinformación. El requisito de etiquetar los contenidos generados por sistemas de IA con arreglo al presente Reglamento se entiende sin perjuicio de la obligación establecida en el artículo 16, apartado 6, del Reglamento 2022/2065 de que los proveedores de servicios de alojamiento tramiten las notificaciones sobre contenidos ilícitos recibidas de conformidad con el artículo 16, apartado 1, y no debe influir en la evaluación y la decisión sobre la ilicitud de los contenidos específicos. Dicha evaluación debe realizarse únicamente con referencia a las normas que rigen la legalidad del contenido.

(70 sexies) El cumplimiento de las obligaciones de transparencia para los sistemas de inteligencia artificial contemplados en el presente Reglamento no debe interpretarse como una indicación de que el uso del sistema o de sus resultados es lícito en virtud del presente Reglamento o de otros actos legislativos de la Unión o de los Estados miembros, y debe entenderse sin perjuicio de otras obligaciones de transparencia para los implantadores de sistemas de inteligencia artificial establecidas en el Derecho de la Unión o nacional.

(69) La inteligencia artificial es una familia de tecnologías en rápido desarrollo que requiere una supervisión reglamentaria y un espacio seguro y controlado para la experimentación, garantizando al mismo tiempo una innovación responsable y la integración de salvaguardias adecuadas y medidas de mitigación de riesgos. Para garantizar un marco jurídico que promueva la innovación, esté preparado para el futuro y sea resistente a las perturbaciones, los Estados miembros deben velar por que sus autoridades nacionales competentes establezcan al menos un espacio regulador de la inteligencia artificial a nivel nacional para facilitar el desarrollo y la experimentación de sistemas innovadores de inteligencia artificial bajo una estricta supervisión reglamentaria antes de que estos sistemas se comercialicen o se pongan en servicio de otro modo. Los Estados miembros también podrían cumplir esta obligación participando en los espacios aislados de regulación ya existentes o estableciendo conjuntamente un espacio aislado de regulación con una o varias autoridades competentes de los Estados miembros, en la medida en que esta participación proporcione un nivel equivalente de cobertura nacional para los Estados miembros participantes. Los compartimentos estancos reguladores pueden establecerse en forma física, digital o híbrida y pueden dar cabida tanto a productos físicos como digitales. Las autoridades encargadas de su creación también deberán garantizar que los compartimentos estancos de regulación dispongan de los recursos adecuados para su funcionamiento, incluidos los recursos financieros y humanos.

(70) Los objetivos de los espacios aislados de regulación de la IA deben ser fomentar la innovación en materia de IA mediante el establecimiento de un entorno controlado de experimentación y ensayo en la fase de desarrollo y de precomercialización con vistas a garantizar la conformidad de los sistemas innovadores de IA con el presente Reglamento y demás legislación pertinente de la Unión y de los Estados miembros, mejorar la seguridad jurídica de los innovadores y la supervisión y comprensión por parte de las autoridades competentes de las oportunidades, los riesgos emergentes y las repercusiones del uso de la IA, facilitar el aprendizaje normativo para

las autoridades y las empresas, también con vistas a futuras adaptaciones del marco jurídico, para apoyar la cooperación y el intercambio de buenas prácticas con las autoridades que participan en el espacio aislado de regulación de la IA, y para acelerar el acceso a los mercados, también mediante la eliminación de obstáculos para las pequeñas y medianas empresas (PYME), incluidas las de nueva creación.

Los espacios aislados de regulación deben estar ampliamente disponibles en toda la Unión, y debe prestarse especial atención a su accesibilidad para las PYME, incluidas las nuevas empresas. La participación en el espacio aislado de regulación de la IA debe centrarse en cuestiones que planteen inseguridad jurídica a los proveedores y posibles proveedores para innovar, experimentar con la IA en la Unión y contribuir al aprendizaje normativo basado en pruebas. Por tanto, la supervisión de los sistemas de IA en el espacio aislado regulador de la IA debe abarcar su desarrollo, formación, ensayo y validación antes de que los sistemas se introduzcan en el mercado o se pongan en servicio, así como la noción y ocurrencia de modificaciones sustanciales que puedan requerir un nuevo procedimiento de evaluación de la conformidad. Cuando proceda, las autoridades nacionales competentes que establezcan entornos aislados de regulación de la IA deben cooperar con otras autoridades pertinentes, incluidas las que supervisan la protección de los derechos fundamentales, y podrían permitir la participación de otros agentes del ecosistema de la IA, como las organizaciones nacionales o europeas de normalización, los organismos notificados, las instalaciones de ensayo y experimentación, los laboratorios de investigación y experimentación, los centros europeos de innovación digital y las organizaciones pertinentes de las partes interesadas y de la sociedad civil. Para garantizar una aplicación uniforme en toda la Unión y economías de escala, conviene establecer normas comunes para la aplicación de los entornos aislados reguladores y un marco de cooperación entre las autoridades pertinentes que participan en la supervisión de los entornos aislados. Los compartimentos estancos reguladores de la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otra legislación que permita el establecimiento de otros compartimentos estancos destinados a garantizar el cumplimiento de otra legislación distinta del presente Reglamento. Cuando proceda, las autoridades competentes pertinentes encargadas de esos otros entornos aislados de regulación deben considerar las ventajas de utilizarlos también para garantizar la conformidad de los sistemas de IA con el presente Reglamento. Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio aislado de regulación de la IA, también podrán realizarse y supervisarse pruebas en condiciones reales en el marco del espacio aislado de regulación de la IA.

(72 bis) El presente Reglamento debe proporcionar la base jurídica para que los proveedores y posibles proveedores del espacio aislado de regulación de la IA utilicen los datos personales recogidos con otros fines para

desarrollar determinados sistemas de IA en el interés público dentro del espacio aislado de regulación de la IA, únicamente en condiciones especificadas, en consonancia con el artículo 6, apartado 4, y el artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679, y los artículos 5, 6 y 10 del Reglamento (UE) 2018/1725, y sin perjuicio de los artículos 4, apartado 2, y 10 de la Directiva (UE) 2016/680. Todas las demás obligaciones de los responsables del tratamiento y los derechos de los interesados en virtud del Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 y la Directiva (UE) 2016/680 siguen siendo aplicables. En particular, el presente Reglamento no debe proporcionar una base jurídica en el sentido del artículo 22, apartado 2, letra b), del Reglamento (UE) 2016/679 y del artículo 24, apartado 2, letra b), del Reglamento (UE) 2018/1725. Los proveedores y posibles proveedores del espacio aislado deben garantizar las salvaguardias adecuadas y cooperar con las autoridades competentes, en particular siguiendo sus orientaciones y actuando con celeridad y de buena fe para mitigar adecuadamente los riesgos significativos identificados para la seguridad, la salud y los derechos fundamentales que puedan surgir durante el desarrollo, las pruebas y la experimentación en el espacio aislado.

(72 ter) Con el fin de acelerar el proceso de desarrollo y comercialización de los sistemas de IA de alto riesgo enumerados en el anexo III, es importante que los proveedores o posibles proveedores de tales sistemas puedan también beneficiarse de un régimen específico para probar dichos sistemas en condiciones del mundo real, sin participar en un espacio aislado de regulación de la IA. Sin embargo, en tales casos y teniendo en cuenta las posibles consecuencias de tales pruebas para las personas, debe garantizarse que el Reglamento introduzca garantías y condiciones adecuadas y suficientes para los proveedores o posibles proveedores. Dichas garantías deben incluir, entre otras, la solicitud del consentimiento informado de las personas físicas para participar en las pruebas en condiciones del mundo real, con la excepción de las fuerzas y cuerpos de seguridad en los casos en que la solicitud del consentimiento informado impidiera que se probara el sistema de IA. El consentimiento de los sujetos para participar en dichas pruebas con arreglo al presente Reglamento es distinto y no prejuzga el consentimiento de los interesados para el tratamiento de sus datos personales con arreglo a la legislación pertinente en materia de protección de datos. También es importante minimizar los riesgos y permitir la supervisión por parte de las autoridades competentes y, por lo tanto, exigir a los posibles proveedores que presenten un plan de pruebas en condiciones reales a la autoridad competente de vigilancia del mercado, que registren las pruebas en secciones específicas de la base de datos a escala de la UE, con algunas excepciones limitadas, que establezcan limitaciones sobre el período durante el cual pueden realizarse las pruebas y que exijan salvaguardias adicionales para las personas pertenecientes a determinados grupos vulnerables, así como un acuerdo por escrito en el que se definan las funciones y responsabilidades de los posibles proveedores e implantadores y la supervisión efectiva por parte del personal competente que participe en las pruebas en condiciones reales. Además, conviene prever salvaguardias adicionales para garantizar que las predicciones, recomendaciones o

las decisiones del sistema de IA puedan ser efectivamente anuladas e ignoradas y que los datos personales estén protegidos y se supriman cuando los sujetos hayan retirado su consentimiento para participar en las pruebas, sin perjuicio de sus derechos como interesados en virtud de la legislación de la UE sobre protección de datos. Por lo que se refiere a la transferencia de datos, también conviene prever que los datos recogidos y tratados a efectos de las pruebas en condiciones del mundo real solo se transfieran a terceros países fuera de la Unión siempre que se apliquen las salvaguardias adecuadas y aplicables en virtud del Derecho de la Unión, en particular de conformidad con las bases para la transferencia de datos personales en virtud del Derecho de la Unión sobre protección de datos, mientras que para los datos no personales se establezcan las salvaguardias adecuadas de conformidad con el Derecho de la Unión, como la Ley de gobernanza de datos y la Ley de datos.

(72 quater) Para garantizar que la Inteligencia Artificial conduzca a resultados social y ambientalmente beneficiosos , se anima a los Estados miembros a que apoyen y promuevan la investigación y el desarrollo de soluciones de IA en apoyo de resultados social y ambientalmente beneficiosos, como soluciones basadas en la IA para aumentar la accesibilidad de las personas con discapacidad, abordar las desigualdades socioeconómicas o cumplir objetivos medioambientales, asignando recursos suficientes, incluida financiación pública y de la Unión, y, cuando proceda y siempre que se cumplan los criterios de admisibilidad y selección, considerando en particular proyectos que persigan tales objetivos. Dichos proyectos deberían basarse en el principio de cooperación interdisciplinar entre desarrolladores de IA, expertos en desigualdad y no discriminación, accesibilidad, derechos de los consumidores, medioambientales y digitales, así como académicos.

(71) Para promover y proteger la innovación, es importante que se tengan especialmente en cuenta los intereses de las PYME, incluidas las de nueva creación, que son proveedoras o implantadoras de sistemas de IA. Con este objetivo, los Estados miembros deben desarrollar iniciativas dirigidas a estos operadores, que incluyan la sensibilización y la comunicación de información. Los Estados miembros proporcionarán a las PYME, incluidas las de nueva creación, que tengan un domicilio social o una sucursal en la Unión, acceso prioritario a los entornos aislados reguladores de la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección y sin impedir que otros proveedores y posibles proveedores accedan a los entornos aislados siempre que cumplan las mismas condiciones y criterios. Los Estados miembros utilizarán los canales existentes y, cuando proceda, establecerán nuevos canales específicos para la comunicación con las PYME, las empresas de nueva creación, los implantadores, otros innovadores y, en su caso, las autoridades públicas locales, con el fin de apoyar a las PYME a lo largo de su trayectoria de desarrollo, proporcionándoles orientación y respondiendo a sus preguntas sobre la aplicación del presente Reglamento. Cuando proceda, estos canales trabajarán juntos para crear sinergias y garantizar la homogeneidad de sus orientaciones a las PYME, incluidas las empresas de nueva creación.

e implantadores. Además, los Estados miembros deben facilitar la participación de las PYME y otras partes interesadas en los procesos de desarrollo de la normalización. Por otra parte, cuando los organismos notificados fijen las tasas de evaluación de la conformidad, deberán tenerse en cuenta los intereses y necesidades específicos de las PYME, incluidas las empresas de nueva creación. La Comisión debería evaluar periódicamente los costes de certificación y conformidad para las PYME, incluidas las de nueva creación, mediante consultas transparentes a los usuarios, y debería trabajar con los Estados miembros para reducir dichos costes. Por ejemplo, los costes de traducción relacionados con la documentación obligatoria y la comunicación con las autoridades pueden constituir un coste significativo para los proveedores y otros operadores, especialmente los de menor escala. Es posible que los Estados miembros deban garantizar que una de las lenguas determinadas y aceptadas por ellos para la documentación pertinente de los proveedores y para la comunicación con los operadores sea una que comprenda ampliamente el mayor número posible de implantadores transfronterizos. Con el fin de atender las necesidades específicas de las PYME, incluidas las de nueva creación, la Comisión debe proporcionar plantillas normalizadas para los ámbitos cubiertos por el presente Reglamento a petición del Consejo de AI. Además, la Comisión debe complementar los esfuerzos de los Estados miembros proporcionando una plataforma de información única con información fácil de usar en relación con el presente Reglamento para todos los proveedores e implantadores, organizando campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento, y evaluando y promoviendo la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA. Las medianas empresas que hayan pasado recientemente de la categoría de pequeñas a la de medianas empresas en el sentido del anexo de la Recomendación 2003/361/CE (artículo 16) deberían tener acceso a estas medidas de apoyo, ya que estas nuevas medianas empresas pueden carecer a veces de los recursos jurídicos y la formación necesarios para garantizar una comprensión y un cumplimiento adecuados de las disposiciones.

(73 bis)Con el fin de promover y proteger la innovación, la plataforma de IA a la carta, todos los programas y proyectos de financiación pertinentes de la UE, como el Programa Europa Digital, Horizonte Europa, ejecutados por la Comisión y los Estados miembros a nivel nacional o de la Unión deben contribuir, según proceda, a la consecución de los objetivos del presente Reglamento.

(72) En particular, para minimizar los riesgos de aplicación derivados de la falta de conocimientos y experiencia en el mercado, así como para facilitar el cumplimiento por parte de los proveedores, en particular las PYME, incluidas las empresas de nueva creación, y los organismos notificados de las obligaciones que les impone el presente Reglamento, la plataforma de IA a la carta, los Centros Europeos de Innovación Digital y las instalaciones de ensayo y experimentación establecidas por la Comisión y los Estados miembros a nivel nacional o de la UE deben contribuir a la aplicación del presente Reglamento.

En el marco de su misión y ámbitos de competencia respectivos, pueden prestar, en particular, apoyo técnico y científico a los proveedores y organismos notificados.

(74 bis) Además, con el fin de garantizar la proporcionalidad teniendo en cuenta el tamaño muy pequeño de algunos operadores en relación con los costes de innovación, conviene permitir a las microempresas cumplir una de las obligaciones más costosas, a saber, establecer un sistema de gestión de la calidad, de una manera simplificada que reduciría la carga administrativa y los costes para dichas empresas sin afectar al nivel de protección ni a la necesidad de cumplir los requisitos para los sistemas de IA de alto riesgo. La Comisión debería elaborar directrices para especificar los elementos del sistema de gestión de la calidad que deben cumplir de esta manera simplificada las microempresas.

(73) Conviene que la Comisión facilite, en la medida de lo posible, el acceso a las instalaciones de ensayo y experimentación a los organismos, grupos o laboratorios establecidos o acreditados con arreglo a cualquier legislación de armonización de la Unión pertinente y que desempeñen tareas en el contexto de la evaluación de la conformidad de los productos o dispositivos cubiertos por dicha legislación de armonización de la Unión. Este es el caso, en particular, de los paneles de expertos, los laboratorios de expertos y los laboratorios de referencia en el ámbito de los productos sanitarios de conformidad con el Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746.

(75 bis) El presente Reglamento debe establecer un marco de gobernanza que permita tanto coordinar y apoyar la aplicación del presente Reglamento a nivel nacional, como crear capacidades a nivel de la Unión e integrar a las partes interesadas en el ámbito de la inteligencia artificial. La aplicación y el cumplimiento efectivos del presente Reglamento requieren un marco de gobernanza que permita coordinar y crear competencias centrales a nivel de la Unión. La Comisión ha creado la Oficina de Inteligencia Artificial mediante Decisión de la Comisión de [...], cuya misión consiste en desarrollar los conocimientos especializados y las capacidades de la Unión en el ámbito de la inteligencia artificial y contribuir a la aplicación de la legislación de la Unión sobre inteligencia artificial. Los Estados miembros deben facilitar las tareas de la Oficina de Inteligencia Artificial con vistas a apoyar el desarrollo de los conocimientos y capacidades de la Unión a nivel de la Unión y reforzar el funcionamiento del mercado único digital. Además, debe crearse un Consejo Europeo de Inteligencia Artificial compuesto por representantes de los Estados miembros, un panel científico que integre a la comunidad científica y un foro consultivo que contribuya con aportaciones de las partes interesadas a la aplicación del presente Reglamento, tanto a nivel nacional como de la Unión. El desarrollo de los conocimientos y capacidades de la Unión también debe incluir el aprovechamiento de los recursos y conocimientos existentes, en particular mediante sinergias con las estructuras creadas en el contexto de la aplicación a escala de la Unión de otros actos legislativos y sinergias con iniciativas afines a escala de la Unión.

como la empresa común EuroHPC y las instalaciones de ensayo y experimentación de IA del Programa Europa Digital.

(74) Para facilitar una aplicación fluida, eficaz y armonizada del presente Reglamento, debe crearse un Consejo Europeo de Inteligencia Artificial. La Junta debe reflejar los diversos intereses del ecosistema de la IA y estar compuesta por representantes de los Estados miembros. El Consejo debe ser responsable de una serie de tareas consultivas, entre ellas emitir dictámenes, recomendaciones, asesoramiento o contribuir a la orientación sobre asuntos relacionados con la aplicación del presente Reglamento, incluidas las cuestiones de ejecución, las especificaciones técnicas o las normas existentes relativas a los requisitos establecidos en el presente Reglamento, y asesorar a la Comisión y a los Estados miembros y a sus autoridades nacionales competentes sobre cuestiones específicas relacionadas con la inteligencia artificial. Para dar cierta flexibilidad a los Estados miembros en la designación de sus representantes en el Consejo de Inteligencia Artificial, dichos representantes podrán ser cualesquiera personas pertenecientes a entidades públicas que deben tener las competencias y facultades pertinentes para facilitar la coordinación a nivel nacional y contribuir a la realización de las tareas del Consejo. El Consejo debe crear dos subgrupos permanentes que sirvan de plataforma para la cooperación y el 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. El subgrupo permanente de vigilancia del mercado debe actuar como Grupo de Cooperación Administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020. En consonancia con la función y las tareas de la Comisión de conformidad con el artículo 33 del Reglamento (UE) 2019/1020, la Comisión debe apoyar las actividades del subgrupo permanente de vigilancia del mercado mediante la realización de evaluaciones o estudios de mercado, en particular con vistas a determinar los aspectos del presente Reglamento que requieran una coordinación específica y urgente entre las autoridades de vigilancia del mercado. El Consejo podrá crear otros subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas. El Consejo también debe cooperar, según proceda, con los organismos, grupos de expertos y redes pertinentes de la UE activos en el contexto de la legislación pertinente de la UE, incluidos, en particular, los activos en virtud de la normativa pertinente de la UE sobre datos, productos y servicios digitales.

(76x) Con vistas a garantizar la participación de las partes interesadas en la ejecución y aplicación del presente Reglamento, debe crearse un foro consultivo que asesore y aporte conocimientos técnicos a la Junta Directiva y a la Comisión. Garantizar una representación variada y equilibrada de las partes interesadas entre intereses comerciales y no comerciales y, dentro de la categoría de intereses comerciales, con respecto a las PYME y otras empresas,

el foro consultivo debería incluir, entre otros, a la industria, las empresas emergentes, las PYME, el mundo académico, la sociedad civil, incluidos los interlocutores sociales, así como la Agencia de los Derechos Fundamentales, la Agencia de Ciberseguridad de la Unión Europea, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicación (ETSI).

(76 sexvicies) Para apoyar la aplicación y el cumplimiento del presente Reglamento, en particular las actividades de supervisión de la Oficina de IA por lo que respecta a los modelos de IA de uso general, debe crearse un grupo científico de expertos independientes. Los expertos independientes que constituyan el panel científico deben ser seleccionados sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la inteligencia artificial y deben desempeñar sus tareas con imparcialidad y objetividad y garantizar la confidencialidad de la información y los datos obtenidos en el desempeño de sus tareas y actividades. Para permitir el refuerzo de las capacidades nacionales necesarias para la aplicación efectiva del presente Reglamento, los Estados miembros deben poder solicitar el apoyo del grupo de expertos que constituye el panel científico para sus actividades de aplicación.

(76 bis)Para apoyar una aplicación adecuada en lo que respecta a los sistemas de IA y reforzar las capacidades de los Estados miembros, deben crearse estructuras de apoyo a las pruebas de IA de la UE y ponerlas a disposición de los Estados miembros.

(75) Los Estados miembros desempeñan un papel clave en la aplicación y ejecución del presente Reglamento. A este respecto, cada Estado miembro debe designar al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes a efectos de la supervisión de la aplicación y ejecución del presente Reglamento. Los Estados miembros podrán decidir designar cualquier tipo de entidad pública para desempeñar las funciones de las autoridades nacionales competentes en el sentido del presente Reglamento, de acuerdo con sus características y necesidades organizativas nacionales específicas. Para aumentar la eficacia organizativa por parte de los Estados miembros y establecer un único punto de contacto con el público y otros interlocutores a nivel de los Estados miembros y de la Unión, cada Estado miembro debe designar una autoridad de vigilancia del mercado que actúe como punto de contacto único.

(77 bis) Las autoridades nacionales competentes deben ejercer sus competencias con independencia, imparcialidad y sin prejuicios, a fin de salvaguardar los principios de objetividad de sus actividades y tareas y garantizar la aplicación y ejecución del presente Reglamento. Los miembros de estas autoridades deben abstenerse de toda acción incompatible con sus funciones y deben estar sujetos a las normas de confidencialidad previstas en el presente Reglamento.

Con el fin de garantizar que los proveedores de sistemas de IA de alto riesgo puedan tener en cuenta la experiencia sobre el uso de sistemas de IA de alto riesgo para mejorar sus sistemas y el proceso de diseño y desarrollo o puedan tomar cualquier posible medida correctiva de manera oportuna, todos los proveedores deben contar con un sistema de seguimiento posterior a la comercialización. Cuando proceda, el seguimiento posterior a la comercialización deberá incluir un análisis de la interacción con otros sistemas de IA, incluidos otros dispositivos y programas informáticos. El seguimiento posterior a la comercialización no debe abarcar los datos operativos sensibles de los implantadores que sean autoridades policiales. Este sistema también es clave para garantizar que los posibles riesgos que surjan de los sistemas de IA que siguen "aprendiendo" después de su comercialización o puesta en servicio puedan abordarse de manera más eficiente y oportuna. En este contexto, también debe exigirse a los proveedores que dispongan de un sistema para notificar a las autoridades pertinentes cualquier incidente grave derivado del uso de sus sistemas de IA, es decir, incidentes o fallos de funcionamiento que provoquen la muerte o daños graves para la salud, perturbaciones graves e irreversibles de la gestión y el funcionamiento de infraestructuras críticas, incumplimientos de las obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales o daños graves a la propiedad o al medio ambiente.

(76) A fin de garantizar una aplicación adecuada y efectiva de los requisitos y obligaciones establecidos por el presente Reglamento, que es legislación de armonización de la Unión, debe aplicarse en su totalidad el sistema de vigilancia del mercado y conformidad de los productos establecido por el Reglamento (UE) 2019/1020. Las autoridades de vigilancia del mercado designadas de conformidad con el presente Reglamento deben tener todas las competencias de ejecución en virtud del presente Reglamento y del Reglamento (UE) 2019/1020 y deben ejercer sus competencias y desempeñar sus funciones de forma independiente, imparcial y sin sesgos. Aunque la mayoría de los sistemas de IA no están sujetos a requisitos y obligaciones específicos en virtud del presente Reglamento, las autoridades de vigilancia del mercado pueden adoptar medidas en relación con todos los sistemas de IA cuando presenten un riesgo de conformidad con el presente Reglamento. Debido a la naturaleza específica de las instituciones, agencias y organismos de la Unión que entran en el ámbito de aplicación del presente Reglamento, procede designar al Supervisor Europeo de Protección de Datos como autoridad de vigilancia del mercado competente para ellos. Ello debe entenderse sin perjuicio de la designación de autoridades nacionales competentes por parte de los Estados miembros. Las actividades de vigilancia del mercado no deben afectar a la capacidad de las entidades supervisadas para llevar a cabo sus tareas de forma independiente, cuando dicha independencia sea exigida por el Derecho de la Unión.

(79 bis) El presente Reglamento se entiende sin perjuicio de las competencias, funciones, facultades e independencia de las autoridades u organismos públicos nacionales pertinentes que supervisan la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de igualdad y protección de datos.

autoridades. Cuando sea necesario para su mandato, dichas autoridades u organismos públicos nacionales también deben tener acceso a cualquier documentación creada en virtud del presente Reglamento. Debe establecerse un procedimiento de salvaguardia específico para garantizar una aplicación adecuada y oportuna contra los sistemas de IA que presenten un riesgo para la salud, la seguridad y los derechos fundamentales. El procedimiento para los sistemas de IA que presenten un riesgo debe aplicarse a los sistemas de IA de alto riesgo que presenten un riesgo, a los sistemas prohibidos que se hayan comercializado, puesto en servicio o utilizado infringiendo las prácticas prohibidas establecidas en el presente Reglamento y a los sistemas de IA que se hayan puesto a disposición infringiendo los requisitos de transparencia establecidos en el presente Reglamento y presenten un riesgo.

(77) La legislación de la Unión en materia de servicios financieros incluye normas y requisitos de gobernanza interna y gestión de riesgos que son aplicables a las entidades financieras reguladas en el marco de la prestación de dichos servicios, incluso cuando hacen uso de sistemas de IA. A fin de garantizar la aplicación y el cumplimiento coherentes de las obligaciones derivadas del presente Reglamento y de las normas y requisitos pertinentes de la legislación de la Unión en materia de servicios financieros, las autoridades competentes para la supervisión y el cumplimiento de la legislación en materia de servicios financieros, en particular las autoridades competentes definidas en la Directiva 2009/138/CE, la Directiva (UE) 2016/97, la Directiva 2013/36/UE el Reglamento (UE) nº 575/2013, la Directiva 2008/48/CE y la Directiva 2014/17/UE del Parlamento Europeo y del Consejo, deben ser designadas, en el marco de sus respectivas competencias, como autoridades competentes a efectos de la supervisión de la aplicación del presente Reglamento, incluidas las actividades de vigilancia del mercado, por lo que respecta a los sistemas de IA proporcionados o utilizados por las entidades financieras reguladas y supervisadas, a menos que los Estados miembros decidan designar a otra autoridad para desempeñar estas tareas de vigilancia del mercado. Dichas autoridades competentes deben tener todas las competencias previstas en el presente Reglamento y en el Reglamento (UE) 2019/1020 sobre vigilancia del mercado para hacer cumplir los requisitos y obligaciones del presente Reglamento, incluidas las competencias para llevar a cabo nuestras actividades de vigilancia del mercado a posteriori que puedan integrarse, según proceda, en sus mecanismos y procedimientos de supervisión existentes en virtud de la legislación pertinente de la Unión en materia de servicios financieros. Conviene prever que, cuando actúen como autoridades de vigilancia del mercado en virtud del presente Reglamento, las autoridades nacionales responsables de la supervisión de las entidades de crédito reguladas con arreglo a la Directiva 2013/36/UE, que participen en el Mecanismo Único de Supervisión (MUS) establecido por el Reglamento (UE) n.º 1024/2013 del Consejo, comuniquen sin demora al Banco Central Europeo toda información detectada en el curso de sus actividades de vigilancia del mercado que pueda ser de interés potencial para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento. Para reforzar aún más la

coherencia entre el presente Reglamento y las normas aplicables a las entidades de crédito reguladas en virtud de la Directiva 2013/36/UE del Parlamento Europeo y del Consejo[27] , conviene asimismo integrar algunas de las obligaciones de procedimiento de los proveedores en relación con la gestión de riesgos, la supervisión posterior a la comercialización y la documentación en las obligaciones y procedimientos existentes en virtud de la Directiva 2013/36/UE. A fin de evitar solapamientos, también deben preverse excepciones limitadas en relación con el sistema de gestión de la calidad de los proveedores y la obligación de supervisión impuesta a los implantadores de sistemas de IA de alto riesgo en la medida en que se apliquen a las entidades de crédito reguladas por la Directiva 2013/36/UE. El mismo régimen debe aplicarse a las empresas de seguros y de reaseguros y a las sociedades de cartera de seguros con arreglo a la Directiva 2009/138/UE (Solvencia II) y a los intermediarios de seguros con arreglo a la Directiva 2016/97/UE y a otros tipos de entidades financieras sujetas a requisitos en materia de gobernanza interna, disposiciones o procesos establecidos de conformidad con la legislación pertinente de la Unión sobre servicios financieros para garantizar la coherencia y la igualdad de trato en el sector financiero.

(80-x) Cada autoridad de vigilancia del mercado para los sistemas de IA de alto riesgo enumerados en el punto 1 del anexo III, en la medida en que estos sistemas se utilicen con fines policiales y para los fines enumerados en los puntos 6, 7 y 8 del anexo III, debe tener poderes efectivos de investigación y corrección, incluida al menos la facultad de obtener acceso a todos los datos personales que se estén tratando y a toda la información necesaria para el desempeño de sus funciones. Las autoridades de vigilancia del mercado deben poder ejercer sus poderes actuando con total independencia. Cualquier limitación de su acceso a datos operativos sensibles en virtud del presente Reglamento debe entenderse sin perjuicio de las competencias que les confiere la Directiva 2016/680. Ninguna exclusión sobre la divulgación de datos a las autoridades nacionales de protección de datos en virtud del presente Reglamento debe afectar a las competencias actuales o futuras de dichas autoridades más allá del ámbito de aplicación del presente Reglamento.

(80 quinvicies) Las autoridades de vigilancia del mercado de los Estados miembros y la Comisión deben poder proponer actividades conjuntas, incluidas investigaciones conjuntas, que lleven a cabo las autoridades de vigilancia del mercado o las autoridades de vigilancia del mercado conjuntamente con la Comisión, que tengan por objeto promover el cumplimiento, detectar el incumplimiento, aumentar la sensibilización y proporcionar orientación en relación con el presente Reglamento con respecto a categorías específicas de sistemas de IA de alto riesgo que se considere que presentan un riesgo grave en varios Estados miembros.

---

[27] Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

Las actividades conjuntas para promover el cumplimiento deben llevarse a cabo de conformidad con el artículo 9 de la Directiva 2019/1020. La Oficina de AI debe prestar apoyo a la coordinación de las investigaciones conjuntas.

(80 sexvicies) Es necesario aclarar las responsabilidades y competencias a nivel nacional y de la Unión en lo que respecta a los sistemas de IA que se basan en modelos de IA de propósito general. Para evitar el solapamiento de competencias, cuando un sistema de IA se base en un modelo de IA de propósito general y el modelo y el sistema sean suministrados por el mismo proveedor, la supervisión debe tener lugar a nivel de la Unión a través de la Oficina de IA, que debe tener las competencias de una autoridad de vigilancia del mercado en el sentido del Reglamento (UE) 2019/1020 a tal efecto. En todos los demás casos, las autoridades nacionales de vigilancia del mercado siguen siendo responsables de la supervisión de los sistemas de IA. Sin embargo, en el caso de los sistemas de IA de uso general que puedan ser utilizados directamente por los desplegadores para al menos un propósito clasificado como de alto riesgo, las autoridades de vigilancia del mercado deben cooperar con la Oficina de IA para llevar a cabo evaluaciones de cumplimiento e informar al Consejo y a otras autoridades de vigilancia del mercado en consecuencia. Además, las autoridades de vigilancia del mercado deben poder solicitar asistencia a la Oficina de IA cuando la autoridad de vigilancia del mercado no pueda concluir una investigación sobre un sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA de propósito general en el que se basa el sistema de IA de alto riesgo. En tales casos, debe aplicarse por analogía el procedimiento relativo a la asistencia mutua en casos transfronterizos del capítulo VI del Reglamento (UE) 2019/1020.

(80z) Para aprovechar al máximo los conocimientos centralizados de la Unión y las sinergias a escala de la Unión, las competencias de supervisión y ejecución de las obligaciones de los proveedores de modelos de IA de uso general deben ser competencia de la Comisión. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de los poderes de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión basado en los Tratados. La Oficina de IA debe poder llevar a cabo todas las acciones necesarias para supervisar la aplicación efectiva del presente Reglamento en lo que respecta a los modelos de IA de propósito general. Debe poder investigar las posibles infracciones de las normas relativas a los proveedores de modelos de IA de propósito general tanto por iniciativa propia, a raíz de los resultados de sus actividades de supervisión, como a petición de las autoridades de vigilancia del mercado, en consonancia con las condiciones establecidas en el presente Reglamento. Para apoyar una supervisión eficaz de la Oficina de IA, debe prever la posibilidad de que los proveedores intermedios presenten denuncias sobre posibles infracciones de las normas relativas a los proveedores de modelos de IA de propósito general.

(80z+1) Con vistas a complementar los sistemas de gobernanza de los modelos de IA de uso general, el panel científico debe apoyar las actividades de supervisión de la Oficina de IA y puede, en

en determinados casos, proporcionar alertas cualificadas a la Oficina de IA que desencadenen medidas de seguimiento, como investigaciones. Este debería ser el caso cuando el grupo científico tenga motivos para sospechar que un modelo de IA de propósito general plantea un riesgo concreto e identificable a nivel de la Unión.

Además, este debería ser el caso cuando el panel científico tenga motivos para sospechar que un modelo de IA de propósito general cumple los criterios que llevarían a clasificarlo como modelo de IA de propósito general con riesgo sistémico. Para dotar al panel científico de la información necesaria para el desempeño de estas tareas, debe existir un mecanismo por el que el panel científico pueda solicitar a la Comisión que requiera documentación o información de un proveedor.

(80z+2) La Oficina de IA debe poder adoptar las medidas necesarias para supervisar la aplicación efectiva y el cumplimiento de las obligaciones de los proveedores de modelos de IA de propósito general establecidas en el presente Reglamento. La Oficina de IA debe poder investigar posibles infracciones de conformidad con las competencias previstas en el presente Reglamento, incluida la solicitud de documentación e información, la realización de evaluaciones, así como la solicitud de medidas a los proveedores de modelos de IA de propósito general. En la realización de las evaluaciones, con el fin de recurrir a expertos independientes, la Oficina de IA debe poder recurrir a expertos independientes para que realicen las evaluaciones en su nombre. El cumplimiento de las obligaciones debe poder exigirse, entre otras cosas, solicitando la adopción de medidas adecuadas, incluidas medidas de mitigación del riesgo en caso de riesgos sistémicos identificados, así como la restricción de la comercialización, la retirada o la recuperación del modelo. Como salvaguardia en caso necesario más allá de los derechos procedimentales previstos en el presente Reglamento, los proveedores de modelos de IA de propósito general deben tener los derechos procedimentales previstos en el artículo 18 del Reglamento (UE) 2019/1020, que deben aplicarse por analogía, sin perjuicio de los derechos procedimentales más específicos previstos en el presente Reglamento.

(78) El desarrollo de sistemas de IA distintos de los sistemas de IA de alto riesgo de conformidad con los requisitos del presente Reglamento puede conducir a una mayor adopción de la inteligencia artificial ética y fiable en la Unión. Debe alentarse a los proveedores de sistemas de IA que no sean de alto riesgo a crear códigos de conducta, incluidos los mecanismos de gobernanza conexos, destinados a fomentar la aplicación voluntaria de algunos o todos los requisitos obligatorios aplicables a los sistemas de IA de alto riesgo, adaptados a la luz de la finalidad prevista de los sistemas y del menor riesgo que entrañan y teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector, como las tarjetas de modelo y de datos. También debe alentarse a los proveedores y, en su caso, a los implantadores de todos los sistemas de IA, de alto riesgo o no, y modelos a que apliquen de forma voluntaria requisitos adicionales relacionados, por ejemplo, con los elementos de la

Directrices éticas europeas para una IA digna de confianza, sostenibilidad medioambiental, medidas de alfabetización en IA, diseño y desarrollo inclusivos y diversos de los sistemas de IA, incluida la atención a las personas vulnerables y la accesibilidad para las personas con discapacidad, participación de las partes interesadas con la implicación, según proceda, de las partes interesadas pertinentes, como organizaciones empresariales y de la sociedad civil, organizaciones académicas y de investigación, sindicatos y organizaciones de protección de los consumidores, en el diseño y desarrollo de los sistemas de IA, y diversidad de los equipos de desarrollo, incluido el equilibrio de género. Para garantizar la eficacia de los códigos de conducta voluntarios, deben basarse en objetivos claros e indicadores clave de rendimiento para medir la consecución de dichos objetivos. También deben desarrollarse de forma inclusiva, según proceda, con la participación de las partes interesadas pertinentes, como las empresas y las organizaciones de la sociedad civil, el mundo académico y las organizaciones de investigación, los sindicatos y las organizaciones de protección de los consumidores. La Comisión podrá desarrollar iniciativas, incluso de carácter sectorial, para facilitar la reducción de las barreras técnicas que dificultan el intercambio transfronterizo de datos para el desarrollo de la IA, incluidas las relativas a la infraestructura de acceso a los datos y a la interoperabilidad semántica y técnica de los diferentes tipos de datos.

(79) Es importante que los sistemas de IA relacionados con productos que no son de alto riesgo con arreglo al presente Reglamento y que, por tanto, no están obligados a cumplir los requisitos establecidos para los sistemas de IA de alto riesgo sean, no obstante, seguros cuando se comercialicen o se pongan en servicio. Para contribuir a este objetivo, se aplicaría como red de seguridad el Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo[28] .

(80) Con el fin de garantizar una cooperación fiable y constructiva de las autoridades competentes a escala de la Unión y nacional, todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos obtenidos en el desempeño de sus funciones, de conformidad con el Derecho de la Unión o nacional. Deben llevar a cabo sus tareas y actividades de manera que se protejan, en particular, los derechos de propiedad intelectual, la información empresarial confidencial y los secretos comerciales, la aplicación efectiva del presente Reglamento, los intereses de la seguridad pública y nacional, la integridad de los procedimientos penales o administrativos y la integridad de la información clasificada.

(81) El cumplimiento del presente Reglamento debe poder exigirse mediante la imposición de sanciones y otras medidas coercitivas. Los Estados miembros deben adoptar todas las

[28] Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (Texto pertinente a efectos del EEE) (DO L 135 de 23.5.2023, p. 1-51).

medidas para garantizar la aplicación de las disposiciones del presente Reglamento, en particular estableciendo sanciones efectivas, proporcionadas y disuasorias en caso de infracción, y respetando el principio ne bis in idem. Con el fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, deben establecerse los límites máximos para la fijación de las multas administrativas por determinadas infracciones específicas. Al evaluar el importe de las multas, los Estados miembros deben tener en cuenta, en cada caso concreto, todas las circunstancias pertinentes de la situación específica, prestando la debida atención, en particular, a la naturaleza, gravedad y duración de la infracción y de sus consecuencias, así como al tamaño del proveedor, en particular si se trata de una PYME, incluida una empresa de nueva creación. El Supervisor Europeo de Protección de Datos debe estar facultado para imponer multas a las instituciones, agencias y organismos de la Unión que entren en el ámbito de aplicación del presente Reglamento.

(84 bis) El cumplimiento de las obligaciones impuestas a los proveedores de modelos de IA de propósito general en virtud del presente Reglamento debe exigirse, entre otras cosas, mediante multas. A tal fin, también deben establecerse niveles adecuados de multas por incumplimiento de dichas obligaciones, incluido el incumplimiento de las medidas solicitadas por la Comisión de conformidad con el presente Reglamento, sujetas a plazos de prescripción adecuados 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 el TFUE.

(84aa)El Derecho de la Unión y los Derechos nacionales ya ofrecen vías de recurso efectivas a las personas físicas y jurídicas cuyos derechos y libertades se vean perjudicados por el uso de sistemas de IA. Sin perjuicio de dichas vías de recurso, cualquier persona física o jurídica que tenga motivos para considerar que se ha producido una infracción de las disposiciones del presente Reglamento debe tener derecho a presentar una denuncia ante la autoridad de vigilancia del mercado pertinente o ante la Oficina de IA, en su caso.

(84 ter)Las personas afectadas deben tener derecho a solicitar una explicación cuando el responsable del despliegue adopte una decisión con los resultados de determinados sistemas de alto riesgo previstos en el presente Reglamento como base principal y que produzca efectos jurídicos o le afecte significativamente de manera similar de forma que considere que repercute negativamente en su salud, su seguridad o sus derechos fundamentales. Esta explicación debe ser clara y significativa y debe proporcionar una base para que las personas afectadas ejerzan sus derechos. Esto no debe aplicarse al uso de sistemas de IA para los que se deriven excepciones o restricciones de la legislación de la Unión o nacional y sólo debe aplicarse en la medida en que este derecho no esté ya previsto en la legislación de la Unión.

(84 quater) Las personas que actúen como "denunciantes" de infracciones del presente Reglamento deben gozar de la protección garantizada por la legislación de la Unión sobre la protección de las personas que denuncian infracciones de la ley. Por consiguiente, la Directiva (UE) 2019/1937 debe aplicarse a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien dichas infracciones.

(82) A fin de garantizar que el marco reglamentario pueda adaptarse en caso necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE para modificar la legislación de armonización de la Unión enumerada en el anexo II, los sistemas de IA de alto riesgo enumerados en el anexo III, las disposiciones relativas a la documentación técnica enumeradas en el anexo IV, el contenido de la declaración UE de conformidad del anexo V, las disposiciones relativas a los procedimientos de evaluación de la conformidad de los anexos VI y VII, las disposiciones por las que se establecen los sistemas de IA de alto riesgo a los que debe aplicarse el procedimiento de evaluación de la conformidad basado en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica, el umbral, así como para complementar los puntos de referencia e indicadores en las normas de clasificación de los modelos de IA de propósito general con riesgo sistémico, los criterios para la designación de los modelos de IA de propósito general con riesgo sistémico en el anexo IX quater, la documentación técnica para los proveedores de modelos de IA de propósito general en el anexo VIII ter y la información sobre transparencia para los proveedores de modelos de IA de propósito general en el anexo VIII quater. Reviste especial importancia que la Comisión lleve a cabo las consultas apropiadas durante sus trabajos preparatorios, incluso a nivel de expertos, y que dichas consultas se realicen de conformidad con los principios establecidos en el Acuerdo Interinstitucional de 13 de abril de 2016 "Legislar mejor"[1] . En particular, para garantizar la igualdad de participación en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben todos los documentos al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupan de la preparación de los actos delegados.

(85 bis) Habida cuenta de la rápida evolución tecnológica y de los conocimientos técnicos necesarios para la aplicación efectiva del presente Reglamento, la Comisión debe evaluar y revisar el presente Reglamento a más tardar tres años después de la fecha de su entrada en vigor y, posteriormente, cada cuatro años, e informar de ello al Parlamento Europeo y al Consejo. Además, teniendo en cuenta las implicaciones para el ámbito de aplicación del presente Reglamento, la Comisión debe llevar a cabo una evaluación de la necesidad de modificar la lista del anexo III y la lista de prácticas prohibidas una vez al año. Por otra parte, a más tardar dos años después de la entrada en vigor y posteriormente cada cuatro años, la Comisión debe evaluar e informar al Parlamento Europeo y al Consejo sobre la necesidad de modificar las zonas de alto riesgo del anexo III, los sistemas de IA dentro de

el alcance de las obligaciones de transparencia del título IV, la eficacia del sistema de supervisión y gobernanza y los avances en la elaboración de productos de normalización sobre el desarrollo energéticamente eficiente de modelos de IA de propósito general, incluida la necesidad de nuevas medidas o acciones. Por último, en un plazo de dos años a partir de la entrada en aplicación y, posteriormente, cada tres años, la Comisión deberá evaluar el impacto y la eficacia de los códigos de conducta voluntarios para fomentar la aplicación de los requisitos establecidos en el capítulo 2 del título III para los sistemas distintos de los sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para dichos sistemas de IA.

(83) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) no 182/2011 del Parlamento Europeo y del Consejo[1] .

(84) Dado que el objetivo del presente Reglamento no puede ser alcanzado de manera suficiente por los Estados miembros y, por consiguiente, debido a la dimensión o a los efectos de la acción, puede lograrse mejor a escala de la Unión, ésta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(87 bis)Con el fin de garantizar la seguridad jurídica, asegurar un período de adaptación adecuado para los operadores y evitar perturbaciones en el mercado, entre otras cosas garantizando la continuidad del uso de los sistemas de IA, conviene que el presente Reglamento se aplique a los sistemas de IA de alto riesgo que se hayan comercializado o puesto en servicio antes de la fecha general de aplicación del mismo, únicamente si, a partir de esa fecha, dichos sistemas son objeto de cambios significativos en su diseño o finalidad prevista. Conviene aclarar que, a este respecto, el concepto de cambio significativo debe entenderse como equivalente en sustancia a la noción de modificación sustancial, que se utiliza únicamente en relación con los sistemas de IA de alto riesgo definidos en el presente Reglamento. Con carácter excepcional y a la luz de la responsabilidad pública, los operadores de sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en el anexo IX y los operadores de sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas deben adoptar las medidas necesarias para cumplir los requisitos del presente Reglamento antes de finales de 2030 y antes de cuatro años después de su entrada en aplicación, respectivamente.

(87 ter) Se anima a los proveedores de sistemas de IA de alto riesgo a que empiecen a cumplir, con carácter voluntario, las obligaciones pertinentes previstas en el presente Reglamento ya durante el período transitorio.

(85) El presente Reglamento debe aplicarse a partir de ... [OP - insértese la fecha establecida en el artículo 85]. Sin embargo, teniendo en cuenta el riesgo inaceptable asociado al uso de la IA en determinadas formas, las prohibiciones deben aplicarse ya a partir de ... [OP - insértese la fecha - 6 meses después de la entrada en vigor del presente Reglamento]. Si bien el pleno efecto de estas prohibiciones se produce con el establecimiento de la gobernanza y la aplicación del presente Reglamento, anticipar la aplicación de las prohibiciones es importante para tener en cuenta el riesgo inaceptable y tiene efecto en otros procedimientos, como en el Derecho civil. Además, la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad debe estar operativa antes del [OP - insértese la fecha establecida en el artículo 85], por lo que las disposiciones sobre los organismos notificados y la estructura de gobernanza deben aplicarse a partir del ... [OP - insértese la fecha - doce meses después de la entrada en vigor del presente Reglamento]. Dado el rápido ritmo de los avances tecnológicos y la adopción de modelos de IA de propósito general, las obligaciones para los proveedores de modelos de IA de propósito general deben aplicarse en un plazo de doce meses a partir de la fecha de entrada en vigor. Los códigos de buenas prácticas deberían estar listos a más tardar 3 meses antes de la entrada en vigor de las disposiciones pertinentes, para que los proveedores puedan demostrar su cumplimiento a tiempo. La Oficina de AI debe velar por que las normas y procedimientos de clasificación se actualicen a la luz de los avances tecnológicos. Además, los Estados miembros deben establecer y notificar a la Comisión el régimen de sanciones, incluidas las multas administrativas, y velar por su correcta y efectiva aplicación en la fecha de entrada en vigor del presente Reglamento. Por consiguiente, las disposiciones sobre sanciones deben aplicarse a partir del [OP - insértese la fecha - doce meses después de la entrada en vigor del presente Reglamento].

(86) El Supervisor Europeo de Protección de Datos y el Consejo Europeo de Protección de Datos fueron consultados de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725 y emitieron un dictamen el 18 de junio de 2021.

TÍTULO I DISPOSICIONES GENERALES

Artículo 1

**Asunto**

1. El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de la inteligencia artificial centrada en el ser humano y digna de confianza, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad, los derechos fundamentales consagrados en la Carta, incluida la democracia, el Estado de Derecho y la protección del medio ambiente contra los efectos nocivos de los sistemas de inteligencia artificial en la Unión y apoyando la innovación.

2. El presente Reglamento establece:

(a) normas armonizadas para la comercialización, la puesta en servicio y el uso de sistemas de inteligencia artificial ("sistemas de IA") en la Unión;

(b) prohibición de determinadas prácticas de inteligencia artificial;

(c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;

(d) normas de transparencia armonizadas para determinados sistemas de IA;

(d bis) normas armonizadas para la comercialización de modelos de IA de uso general;

(e) normas sobre supervisión del mercado, gobernanza de la vigilancia del mercado y aplicación;

(ea) medidas de apoyo a la innovación, con especial atención a las PYME, incluidas las de nueva creación.

Artículo 2

**Alcance**

1. El presente Reglamento se aplica a:

(a) proveedores que comercialicen o pongan en servicio sistemas de IA o comercialicen modelos de IA de uso general en la Unión, con independencia de que dichos proveedores estén establecidos o ubicados en la Unión o en un tercer país;

desplegadores de sistemas de IA que tengan su lugar de establecimiento o que estén situados en la Unión;

(b) proveedores e implantadores de sistemas de IA que tengan su lugar de establecimiento o estén situados en un tercer país, cuando el producto generado por el sistema se utilice en la Unión;

(c bis) importadores y distribuidores de sistemas de IA;

(c ter) fabricantes de productos que comercializan o ponen en servicio un sistema de IA junto con su producto y bajo su propio nombre o marca;

(cc) representantes autorizados de proveedores que no estén establecidos en la Unión. (cc) personas afectadas que estén establecidas en la Unión.

2. Para los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartados 1 y 2, relacionados con productos cubiertos por la legislación de armonización de la Unión enumerada en el anexo II, sección B, sólo se aplicará el artículo 84 del presente Reglamento. El artículo 53 se aplicará únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo con arreglo al presente Reglamento se hayan integrado en dicha legislación de armonización de la Unión.

3. El presente Reglamento no se aplicará a los ámbitos ajenos al Derecho de la UE y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado la realización de las tareas relacionadas con dichas competencias.

El presente Reglamento no se aplicará a los sistemas de IA en la medida en que se comercialicen, se pongan en servicio o se utilicen, con o sin modificación de dichos sistemas, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo dichas actividades.

El presente Reglamento no se aplicará a los sistemas de IA que no se comercialicen ni se pongan en servicio en la Unión, cuando la producción se utilice en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo dichas actividades.

4. 2. El presente Reglamento no se aplicará a las autoridades públicas de un tercer país ni a las organizaciones internacionales incluidas en el ámbito de aplicación del presente Reglamento con arreglo al apartado 1, cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de la cooperación internacional o de acuerdos de cooperación policial y judicial con la Unión o con uno o varios Estados miembros, a condición de que dicho tercer país o

las organizaciones internacionales ofrezcan garantías adecuadas con respecto a la protección de los derechos y libertades fundamentales de las personas.

5. El presente Reglamento no afectará a la aplicación de las disposiciones sobre la responsabilidad de los proveedores de servicios intermediarios establecidas en el capítulo II, sección 4, de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo[29] [que *será sustituida por las disposiciones correspondientes de la Ley de Servicios Digitales*].

5 bis. El presente Reglamento no se aplicará a los sistemas y modelos de IA, incluidos sus resultados, específicamente desarrollados y puestos en servicio con el único fin de la investigación y el desarrollo científicos.

5 bis.El Derecho de la Unión en materia de protección de datos personales, privacidad y confidencialidad de las comunicaciones se aplica a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 ni a las Directivas 2002/58/CE y (UE) 2016/680, sin perjuicio de lo dispuesto en el artículo 10, apartado 5, y en el artículo 54 del presente Reglamento.

5 ter. El presente Reglamento no se aplicará a ninguna actividad de investigación, ensayo y desarrollo relativa a sistemas o modelos de IA antes de su comercialización o puesta en servicio; dichas actividades se llevarán a cabo respetando la legislación aplicable de la Unión. Las pruebas en condiciones reales no estarán cubiertas por esta exención.

5 ter. El presente Reglamento se entiende sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relacionados con la protección de los consumidores y la seguridad de los productos.

5 quáter. El presente Reglamento no se aplicará a las obligaciones de los implantadores que sean personas físicas que utilicen sistemas de IA en el curso de una actividad no profesional puramente personal.

5 sexies. El presente Reglamento no será obstáculo para que los Estados miembros o la Unión mantengan o introduzcan disposiciones legales, reglamentarias o administrativas más favorables para los trabajadores en lo que se refiere a la protección de sus derechos en relación con la utilización de sistemas de IA por parte de los empresarios, o para fomentar o permitir la aplicación de convenios colectivos más favorables para los trabajadores.

---

[29] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior ("Directiva sobre el comercio electrónico") (DO L 178 de 17.7.2000, p. 1).

5 octies. Las obligaciones establecidas en el presente Reglamento no se aplicarán a los sistemas de IA liberados bajo licencias libres y de código abierto, a menos que se comercialicen o se pongan en servicio como sistemas de IA de alto riesgo o un sistema de IA incluido en los títulos II y IV.

*Artículo 3*

**Definiciones**

A efectos del presente Reglamento, se entenderá por

(1) Sistema de IA" es un sistema basado en máquinas diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales;

(1 bis) "riesgo": la combinación de la probabilidad de que se produzca un daño y la gravedad de ese daño;

(2) proveedor": una persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolle un sistema de IA o un modelo de IA de propósito general o que haga desarrollar un sistema de IA o un modelo de IA de propósito general y los comercialice o ponga en servicio bajo su propio nombre o marca comercial, ya sea a título oneroso o gratuito;

(4) Desplegador": cualquier persona física o jurídica, autoridad pública, agencia u otro organismo que utilice un sistema de IA bajo su autoridad, excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional;

(5) representante autorizado": toda persona física o jurídica situada o establecida en la Unión que haya recibido y aceptado un mandato escrito de un proveedor de un sistema de IA o de un modelo de IA de propósito general para, respectivamente, ejecutar y llevar a cabo en su nombre las obligaciones y procedimientos establecidos por el presente Reglamento;

(6) importador": toda persona física o jurídica situada o establecida en la Unión que comercialice un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión;

(7) distribuidor": cualquier persona física o jurídica de la cadena de suministro, distinta del proveedor o del importador, que comercialice un sistema de IA en el mercado de la Unión;

operador": el proveedor, el fabricante del producto, el implantador, el representante autorizado, el importador o el distribuidor;

(8) comercialización": la primera puesta a disposición en el mercado de la Unión de un sistema de IA o de un modelo de IA de propósito general;

(9) puesta a disposición en el mercado": todo suministro de un sistema de IA o de un modelo de IA de propósito general para su distribución o uso en el mercado de la Unión en el curso de una actividad comercial, ya sea a cambio de una remuneración o de forma gratuita;

(10) puesta en servicio": el suministro de un sistema de IA para su primer uso directamente al usuario o para uso propio en la Unión para los fines previstos;

(11) finalidad prevista": el uso al que el proveedor destina un sistema de IA, incluidos el contexto y las condiciones de uso específicos, tal como se especifica en la información facilitada por el proveedor en las instrucciones de uso, el material promocional o de venta y las declaraciones, así como en la documentación técnica;

(12) uso indebido razonablemente previsible": el uso de un sistema de IA de forma no conforme con su finalidad prevista, pero que puede resultar de un comportamiento humano razonablemente previsible o de la interacción con otros sistemas, incluidos otros sistemas de IA;

(13) Componente de seguridad de un producto o sistema": componente de un producto o de un sistema que cumple una función de seguridad para dicho producto o sistema, o cuyo fallo o mal funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes;

(14) instrucciones de uso": la información facilitada por el proveedor para informar al usuario, en particular, de la finalidad prevista y el uso adecuado de un sistema de IA;

(15) retirada de un sistema de IA": cualquier medida destinada a lograr la devolución al proveedor o a ponerlo fuera de servicio o inhabilitar el uso de un sistema de IA puesto a disposición de los implantadores;

(16) retirada de un sistema de IA": cualquier medida destinada a impedir la comercialización de un sistema de IA en la cadena de suministro;

(17) rendimiento de un sistema de inteligencia artificial": la capacidad de un sistema de inteligencia artificial para alcanzar el objetivo previsto;

autoridad notificante": la autoridad nacional responsable de establecer y aplicar los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión;

(18) evaluación de la conformidad": el proceso de demostración del cumplimiento de los requisitos establecidos en el capítulo 2 del título III del presente Reglamento en relación con un sistema de IA de alto riesgo;

(19) organismo de evaluación de la conformidad": un organismo que realiza actividades de evaluación de la conformidad por terceros, incluidos los ensayos, la certificación y la inspección;

(20) organismo notificado": un organismo de evaluación de la conformidad notificado con arreglo al presente Reglamento y a otra legislación pertinente de armonización de la Unión;

(21) modificación sustancial": un cambio en el sistema de IA tras su comercialización o puesta en servicio que no esté previsto o planificado en la evaluación inicial de la conformidad realizada por el proveedor y a resultas del cual se vea afectada la conformidad del sistema de IA con los requisitos establecidos en el título III, capítulo 2, del presente Reglamento o se produzca una modificación de la finalidad prevista para la que se ha evaluado el sistema de IA;

(22) marcado CE de conformidad" (marcado CE): un marcado por el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el título III, capítulo 2, del presente Reglamento y demás legislación aplicable de la Unión por la que se armonizan las condiciones para la comercialización de los productos ("legislación de armonización de la Unión") que prevé su colocación;

(23) sistema de seguimiento poscomercialización": todas las actividades llevadas a cabo por los proveedores de sistemas de IA para recopilar y revisar la experiencia adquirida con el uso de los sistemas de IA que comercializan o ponen en servicio, con el fin de identificar cualquier necesidad de aplicar inmediatamente las medidas correctoras o preventivas necesarias;

(24) "autoridad de vigilancia del mercado": la autoridad nacional que lleva a cabo las actividades y adopta las medidas de conformidad con el Reglamento (UE) 2019/1020;

(25) "norma armonizada": una norma europea tal como se define en el artículo 2, apartado 1, letra c), del Reglamento (UE) no 1025/2012;

(26) "especificación común": un conjunto de especificaciones técnicas, tal como se definen en el artículo 2, punto 4, del Reglamento (UE) no 1025/2012, que proporcionan medios para cumplir determinados requisitos establecidos en virtud del presente Reglamento;

datos de entrenamiento": datos utilizados para entrenar un sistema de IA mediante el ajuste de sus parámetros aprendibles;

(27) datos de validación": datos utilizados para proporcionar una evaluación del sistema de IA entrenado y para ajustar sus parámetros no aprendibles y su proceso de aprendizaje, entre otras cosas, con el fin de evitar un ajuste insuficiente o excesivo; mientras que el conjunto de datos de validación es un conjunto de datos separado o parte del conjunto de datos de entrenamiento, ya sea como una división fija o variable;

(28) datos de ensayo": los datos utilizados para proporcionar una evaluación independiente del sistema de IA con el fin de confirmar el rendimiento esperado de dicho sistema antes de su comercialización o puesta en servicio;

(29) datos de entrada": los datos proporcionados a un sistema de IA o adquiridos directamente por éste, a partir de los cuales el sistema produce un resultado;

(30) datos biométricos": los datos personales resultantes de un tratamiento técnico específico relativo a las características físicas, fisiológicas o de comportamiento de una persona física, como las imágenes faciales o los datos dactiloscópicos;

(33 bis) "identificación biométrica": el reconocimiento automatizado de rasgos humanos físicos, fisiológicos, conductuales y psicológicos con el fin de establecer la identidad de una persona mediante la comparación de datos biométricos de dicha persona con datos biométricos almacenados de personas en una base de datos;

(33 quater) "verificación biométrica": la verificación automatizada de la identidad de las personas físicas mediante la comparación de los datos biométricos de un individuo con datos biométricos facilitados previamente (verificación uno a uno, incluida la autenticación);

(33 quinquies) "categorías especiales de datos personales": las categorías de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725;

(33 sexies) "datos operativos sensibles": los datos operativos relacionados con actividades de prevención, detección, investigación y enjuiciamiento de infracciones penales cuya divulgación pueda poner en peligro la integridad de los procedimientos penales;

(31) sistema de reconocimiento de emociones": un sistema de IA destinado a identificar o deducir emociones o intenciones de personas físicas a partir de sus datos biométricos;

sistema de categorización biométrica": un sistema de IA destinado a asignar personas físicas a categorías específicas sobre la base de sus datos biométricos, a menos que sea auxiliar de otro servicio comercial y estrictamente necesario por razones técnicas objetivas;

(32) sistema de identificación biométrica a distancia": un sistema de IA destinado a identificar a personas físicas, sin su participación activa, normalmente a distancia, mediante la comparación de los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia;

(33) sistema de identificación biométrica a distancia "en tiempo real": un sistema de identificación biométrica a distancia en el que la captura de los datos biométricos, la comparación y la identificación se producen sin demora significativa. Esto incluye no sólo la identificación instantánea, sino también retrasos breves y limitados para evitar la elusión;

(34) sistema de identificación biométrica a distancia "posterior"": un sistema de identificación biométrica a distancia distinto de un sistema de identificación biométrica a distancia "en tiempo real";

(35) espacio de acceso público": cualquier lugar físico de propiedad pública o privada accesible a un número indeterminado de personas físicas, con independencia de que puedan aplicarse determinadas condiciones de acceso y de las posibles restricciones de capacidad;

(36) autoridad encargada de hacer cumplir la ley

(a) cualquier autoridad pública competente en materia de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención de amenazas para la seguridad pública; o

(b) cualquier otro organismo o entidad al que la legislación de un Estado miembro encomiende el ejercicio de la autoridad pública y de los poderes públicos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la salvaguardia y la prevención de amenazas para la seguridad pública;

(37) aplicación de la ley": las actividades llevadas a cabo por las autoridades policiales o judiciales o en su nombre para la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, incluida la protección y prevención de amenazas para la seguridad pública;

Oficina de Inteligencia Artificial": la función de la Comisión de contribuir a la aplicación, el seguimiento y la supervisión de los sistemas de IA, los modelos de IA de propósito general y la gobernanza de la IA. Las referencias del presente Reglamento a la Oficina de Inteligencia Artificial se entenderán hechas a la Comisión;

(38) autoridad nacional competente": cualquiera de las siguientes: la autoridad notificante y la autoridad de vigilancia del mercado. Por lo que respecta a los sistemas de IA puestos en servicio o utilizados por instituciones, agencias, oficinas y organismos de la UE, toda referencia a las autoridades nacionales competentes o a las autoridades de vigilancia del mercado en el presente Reglamento se entenderá hecha al Supervisor Europeo de Protección de Datos;

(39) Incidente grave": cualquier incidente o fallo de funcionamiento de un sistema de IA que provoque directa o indirectamente alguna de las siguientes situaciones:

(a) la muerte de una persona o daños graves para su salud;

(b) una perturbación grave e irreversible de la gestión y el funcionamiento de las infraestructuras críticas;

(b bis) incumplimiento de las obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales; b ter) daños graves a la propiedad o al medio ambiente.

(44 bis) "datos personales": los datos personales definidos en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

(44 quater) "datos no personales": datos distintos de los datos personales definidos en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

(be) "elaboración de perfiles": cualquier forma de tratamiento automatizado de datos personales tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679; o en el caso de las fuerzas y cuerpos de seguridad - en el artículo 3, punto 4, de la Directiva (UE) 2016/680 o, en el caso de las instituciones, órganos u organismos de la Unión, en el artículo 3, punto 5, del Reglamento (UE) 2018/1725;

(bf) "plan de pruebas en condiciones reales": un documento que describe los objetivos, la metodología, el ámbito geográfico, poblacional y temporal, el seguimiento, la organización y la realización de las pruebas en condiciones reales;

(44 septies) "plan del arenero": documento acordado entre el proveedor participante y la autoridad competente en el que se describen los objetivos, las condiciones, el calendario, la metodología y los requisitos de las actividades llevadas a cabo dentro del arenero;

(bg) " espacio aislado regulador de la IA": un marco concreto y controlado establecido por una autoridad competente que ofrece a los proveedores o posibles proveedores de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en su caso en condiciones del mundo real, un sistema de IA innovador, con arreglo a un plan de espacio aislado durante un tiempo limitado bajo supervisión reguladora;

(bh) "alfabetización en materia de IA" se refiere a las capacidades, conocimientos y comprensión que permiten a los proveedores, usuarios y personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, hacer un despliegue informado de los sistemas de IA, así como adquirir conciencia de las oportunidades y riesgos de la IA y de los posibles daños que puede causar;

(bi) "ensayo en condiciones reales": el ensayo temporal de un sistema de IA para su finalidad prevista en condiciones reales fuera de un laboratorio o de un entorno simulado de otro modo, con vistas a recopilar datos fiables y sólidos y a evaluar y verificar la conformidad del sistema de IA con los requisitos del presente Reglamento; el ensayo en condiciones reales no se considerará una comercialización o puesta en servicio del sistema de IA en el sentido del presente Reglamento, siempre que se cumplan todas las condiciones previstas en el artículo 53 o en el artículo 54 bis;

(bj) "sujeto": a efectos de las pruebas en condiciones reales, una persona física que participa en las pruebas en condiciones reales;

(bk) "consentimiento informado": la manifestación libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en un ensayo concreto en condiciones reales, tras haber sido informado de todos los aspectos del ensayo que son relevantes para la decisión del sujeto de participar;

(bl) "deep fake": contenidos de imagen, audio o vídeo generados o manipulados por IA que se asemejan a personas, objetos, lugares u otras entidades o acontecimientos existentes y que a una persona le parecerían falsamente auténticos o veraces;

(44 sexies) "infracción generalizada": cualquier acción u omisión contraria al Derecho de la Unión que proteja los intereses de las personas:

(a) que haya perjudicado o pueda perjudicar los intereses colectivos de personas físicas residentes en al menos dos Estados miembros distintos del Estado miembro, en el que:

(i) se originó o tuvo lugar el acto o la omisión;

se establezca el prestador de que se trate o, en su caso, su representante autorizado, o

(ii) cuando la infracción sea cometida por el ejecutor;

(b) que proteja los intereses de los particulares, que hayan causado, causen o puedan causar perjuicio a los intereses colectivos de los particulares y que presenten características comunes, entre ellas, la misma práctica ilícita, el mismo interés vulnerado y que se produzcan de forma concurrente, cometidas por el mismo operador, en al menos tres Estados miembros;

(44 nonies) "infraestructura crítica": un bien, una instalación, un equipo, una red o un sistema, o una parte del mismo, que sea necesario para la prestación de un servicio esencial en el sentido del artículo 2, apartado 4, de la Directiva (UE) 2022/2557;

(44 ter) "modelo de IA de propósito general": un modelo de IA, incluso cuando se ha entrenado con una gran cantidad de datos utilizando la autosupervisión a escala, que muestra una generalidad significativa y es capaz de realizar de forma competente una amplia gama de tareas distintas, independientemente de la forma en que se comercialice el modelo, y que puede integrarse en una variedad de sistemas o aplicaciones posteriores. Esto no incluye los modelos de IA que se utilizan antes de su comercialización para actividades de investigación, desarrollo y creación de prototipos;

(44 quater) "capacidades de alto impacto" en los modelos de IA de propósito general: capacidades que igualan o superan las capacidades registradas en los modelos de IA de propósito general más avanzados;

(44 quinquies) "riesgo sistémico a nivel de la Unión": un riesgo específico de las capacidades de alto impacto de los modelos de IA de propósito general, que tiene un impacto significativo en el mercado interior debido a su alcance, y con efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a escala a través de la cadena de valor;

(44 sexies) "sistema de IA de propósito general": un sistema de IA que se basa en un modelo de IA de propósito general, que tiene capacidad para servir a diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA;

(44 septies) "operación en coma flotante": cualquier operación matemática o asignación que implique números en coma flotante, que son un subconjunto de los números reales típicamente

representado en los ordenadores por un número entero de precisión fija escalado por un exponente entero de base fija;

(44 octies) "proveedor intermedio": un proveedor de un sistema de IA, incluido un sistema de IA de propósito general, que integra un modelo de IA, con independencia de que el modelo sea proporcionado por ellos mismos e integrado verticalmente o proporcionado por otra entidad sobre la base de relaciones contractuales.

*Artículo 4 ter*

**Alfabetización en IA**

Los proveedores e implantadores de sistemas de IA tomarán medidas para garantizar, en la medida de lo posible, un nivel suficiente de conocimientos de IA de su personal y de otras personas que se ocupen del funcionamiento y uso de los sistemas de IA en su nombre, teniendo en cuenta sus conocimientos técnicos, experiencia, educación y formación y el contexto en el que vayan a utilizarse los sistemas de IA, y considerando las personas o grupos de personas sobre los que vayan a utilizarse los sistemas de IA.

# TÍTULO II
# PRÁCTICAS DE INTELIGENCIA ARTIFICIAL PROHIBIDAS

*Artículo 5*

**Prácticas de inteligencia artificial prohibidas**

1. Quedan prohibidas las siguientes prácticas de inteligencia artificial

(a) la comercialización, puesta en servicio o utilización de un sistema de IA que despliegue técnicas subliminales que escapen a la conciencia de una persona o técnicas deliberadamente manipuladoras o engañosas, con el objetivo o el efecto de distorsionar materialmente el comportamiento de una persona o de un grupo de personas, mermando de forma apreciable la capacidad de la persona para tomar una decisión con conocimiento de causa, haciendo así que la persona tome una decisión que de otro modo no habría tomado, de forma que cause o pueda causar a esa persona, a otra persona o a un grupo de personas un perjuicio importante;

(b) la comercialización, puesta en servicio o utilización de un sistema de IA que explote cualquiera de las vulnerabilidades de una persona o de un grupo específico de personas debido a su edad, discapacidad o una situación social o económica específica, con el objetivo o el efecto de

de distorsionar materialmente el comportamiento de esa persona o de una persona perteneciente a ese grupo de manera que cause o sea razonablemente probable que cause a esa persona o a otra un daño significativo;

(b bis) la comercialización o puesta en servicio con este fin específico, o la utilización de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas basándose en sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual.

Esta prohibición no cubre ningún etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basado en datos biométricos o categorización de datos biométricos en el ámbito de la aplicación de la ley;

(c) la comercialización, puesta en servicio o utilización de sistemas de IA para la evaluación o clasificación de personas físicas o grupos de ellas durante un determinado período de tiempo en función de su comportamiento social o de sus características personales o de personalidad conocidas, inferidas o previstas, con la puntuación social que conduzca a una de las siguientes situaciones o a ambas:

(i) trato perjudicial o desfavorable de determinadas personas físicas o grupos enteros de éstas en contextos sociales que no guardan relación con los contextos en los que se generaron o recopilaron originalmente los datos;

(ii) trato perjudicial o desfavorable a determinadas personas físicas o grupos de éstas, injustificado o desproporcionado a su comportamiento social o a su gravedad;

(d) la utilización de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales, a menos y en la medida en que dicha utilización sea estrictamente necesaria para uno de los objetivos siguientes

(i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos y explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas;

(ii) la prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de las personas físicas o una amenaza real y actual o real y previsible de atentado terrorista;

(iii) la localización o identificación de una persona sospechosa de haber cometido un delito, con el fin de llevar a cabo una investigación penal,

el enjuiciamiento o la ejecución de una sanción penal por delitos contemplados en el anexo II bis y castigados en el Estado miembro de que se trate con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años. El presente apartado se entiende sin perjuicio de lo dispuesto en el artículo 9 del RGPD para el tratamiento de datos biométricos con fines distintos de los policiales.

(d bis) la comercialización, puesta en servicio para este fin específico o utilización de un sistema de IA para realizar evaluaciones de riesgo de personas físicas con el fin de evaluar o predecir el riesgo de que una persona física cometa un delito, basándose únicamente en la elaboración de perfiles de una persona física o en la evaluación de sus rasgos y características de personalidad. Esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la evaluación humana de la implicación de una persona en una actividad delictiva, que ya se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

(d ter) la comercialización, puesta en servicio para este fin específico o utilización de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante el raspado no selectivo de imágenes faciales de Internet o de grabaciones de CCTV;

(dc) la puesta en el mercado, la puesta en servicio con este fin específico o el uso de sistemas de IA para inferir emociones de una persona física en los ámbitos del lugar de trabajo y de las instituciones educativas, excepto en los casos en que el uso del sistema de IA esté destinado a ser puesto en el mercado o en servicio por razones médicas o de seguridad.

1 bis. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de inteligencia artificial infrinja otro Derecho de la Unión.

2. La utilización de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales para cualquiera de los objetivos mencionados en el apartado 1, letra d), sólo se desplegará para los fines previstos en el apartado 1, letra d), para confirmar la identidad de la persona a la que se dirige específicamente, y tendrá en cuenta los siguientes elementos:

(a) la naturaleza de la situación que da lugar a la posible utilización, en particular la gravedad, la probabilidad y la magnitud del perjuicio causado en ausencia de utilización del sistema;

(b) las consecuencias de la utilización del sistema para los derechos y libertades de todas las personas afectadas, en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, la utilización de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales para cualquiera de los objetivos contemplados en la

apartado 1, letra d), deberán cumplir las salvaguardias y condiciones necesarias y proporcionadas en relación con la utilización de conformidad con las legislaciones nacionales que autorizan su uso, en particular en lo que se refiere a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica a distancia "en tiempo real" en espacios de acceso público sólo se autorizará si la autoridad policial ha completado una evaluación de impacto sobre los derechos fundamentales según lo dispuesto en el artículo 29 bis y ha registrado el sistema en la base de datos de conformidad con el artículo 51. No obstante, en casos de urgencia debidamente justificados, podrá iniciarse la utilización del sistema sin el registro, siempre que éste se complete sin demora injustificada.

3. Por lo que se refiere al apartado 1, letra d), y al apartado 2, toda utilización con fines policiales de un sistema de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público estará supeditada a una autorización previa concedida por una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante para el Estado miembro en el que vaya a tener lugar la utilización, emitida previa solicitud motivada y de conformidad con las normas detalladas de Derecho nacional a que se refiere el apartado 4. No obstante, en una situación de urgencia debidamente justificada, podrá iniciarse la utilización del sistema sin autorización, siempre que ésta se solicite sin demora indebida, a más tardar en un plazo de 24 horas. Si se deniega dicha autorización, se interrumpirá su uso con efecto inmediato y todos los datos, así como los resultados y productos de este uso, se desecharán y borrarán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante sólo concederá la autorización cuando esté convencida, basándose en pruebas objetivas o indicios claros que se le presenten, de que el uso del sistema de identificación biométrica a distancia "en tiempo real" en cuestión es necesario y proporcionado para alcanzar uno de los objetivos especificados en el apartado 1, letra d), tal como se identifica en la solicitud y, en particular, se limita a lo estrictamente necesario en cuanto al período de tiempo y al ámbito geográfico y personal. Al decidir sobre la solicitud, la autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante tendrá en cuenta los elementos mencionados en el apartado 2. Se garantizará que la autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante no pueda adoptar ninguna decisión que produzca un efecto jurídico adverso para una persona basándose únicamente en los resultados del sistema de identificación biométrica a distancia.

3 bis. Sin perjuicio de lo dispuesto en el apartado 3, toda utilización de un sistema de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos en

de conformidad con las normas nacionales a que se refiere el apartado 4. La notificación contendrá como mínimo la información especificada en el apartado 5 y no incluirá datos operativos sensibles.

4. Un Estado miembro podrá decidir prever la posibilidad de autorizar total o parcialmente el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales, dentro de los límites y en las condiciones enumeradas en el apartado 1, letra d), y en los apartados 2 y 3. Los Estados miembros interesados establecerán en su legislación nacional las normas detalladas necesarias para la solicitud, la expedición y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como para la supervisión y la presentación de informes al respecto. Dichas normas especificarán asimismo para cuáles de los objetivos enumerados en la letra d) del apartado 1, incluidos los delitos a que se refiere su inciso iii), podrá autorizarse a las autoridades competentes a utilizar dichos sistemas con fines policiales. Los Estados miembros notificarán dichas normas a la Comisión a más tardar 30 días después de su adopción. Los Estados miembros podrán introducir, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica a distancia.

5. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales de conformidad con el apartado 3 bis presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o por una autoridad administrativa independiente cuya decisión sea vinculante para las solicitudes de autorización de conformidad con el apartado 3 y su resultado.

6. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales a partir de datos agregados en los Estados miembros basados en los informes anuales a que se refiere el apartado 5, que no incluirán datos operativos sensibles de las actividades policiales relacionadas.

TÍTULO III

# SISTEMAS DE AI DE ALTO RIESGO

## Capítulo 1

## CLASIFICACIÓN DE LOS SISTEMAS DE AI COMO DE ALTO RIESGO

*Artículo 6*

**Reglas de clasificación de los sistemas de IA de alto riesgo**

1. Con independencia de que un sistema de IA se comercialice o se ponga en servicio independientemente de los productos contemplados en las letras a) y b), dicho sistema de IA se considerará de alto riesgo cuando se cumplan las dos condiciones siguientes:

(a) el sistema de IA está destinado a utilizarse como componente de seguridad de un producto, o el sistema de IA es en sí mismo un producto, cubierto por la legislación de armonización de la Unión enumerada en el anexo II;

(b) el producto cuyo componente de seguridad con arreglo a la letra a) es el sistema de IA, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad por terceros, con vistas a la comercialización o puesta en servicio de dicho producto con arreglo a la legislación de armonización de la Unión enumerada en el anexo II.

2. Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA a que se refiere el anexo III.

2 bis. No obstante lo dispuesto en el apartado 2, los sistemas de IA no se considerarán de alto riesgo si no suponen un riesgo significativo de daño para la salud, la seguridad o los derechos fundamentales de las personas físicas, incluido el hecho de no influir materialmente en el resultado de la toma de decisiones. Este será el caso si se cumplen uno o varios de los siguientes criterios:

(a) el sistema de IA está destinado a realizar una tarea procedimental limitada;

(b) el sistema de IA pretende mejorar el resultado de una actividad humana realizada previamente;

(c) el sistema de IA está destinado a detectar patrones de toma de decisiones o desviaciones de patrones de toma de decisiones anteriores y no está destinado a sustituir o influir en la evaluación humana previamente completada, sin la debida revisión humana; o bien

el sistema de IA está destinado a realizar una tarea preparatoria de una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III.

No obstante lo dispuesto en el párrafo primero del presente apartado, un sistema de IA se considerará siempre de alto riesgo si el sistema de IA realiza la elaboración de perfiles de personas físicas.

2 ter. El proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto riesgo deberá documentar su evaluación antes de que dicho sistema se comercialice o se ponga en servicio.

Dicho proveedor estará sujeto a la obligación de registro establecida en el apartado 1 bis del artículo 51. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación.

2 quáter. La Comisión, previa consulta al Consejo de IA, y a más tardar 18 meses después de la entrada en vigor del presente Reglamento, proporcionará directrices que especifiquen la aplicación práctica del presente artículo, completadas con una lista exhaustiva de ejemplos prácticos de casos de uso de alto riesgo y de no alto riesgo en sistemas de IA, de conformidad con las condiciones establecidas en el artículo 82 bis.

2 quinquies. Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73 a fin de modificar los criterios establecidos en el apartado 2 bis, párrafo primero, letras a) a d).

La Comisión podrá adoptar actos delegados que añadan nuevos criterios a los establecidos en los puntos

(a) a la letra d) del párrafo primero del apartado 2 bis, o modificarlos, únicamente 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 supongan un riesgo significativo de perjuicio para la salud, la seguridad y los derechos fundamentales.

La Comisión adoptará actos delegados por los que se suprima alguno de los criterios establecidos en el apartado 2 bis, párrafo primero, cuando existan pruebas concretas y fiables de que ello es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales en la Unión.

Cualquier modificación de los criterios establecidos en las letras a) a d) del párrafo primero del apartado 2 bis no disminuirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales en la Unión.

Al adoptar los actos delegados, la Comisión garantizará la coherencia con los actos delegados adoptados en virtud del artículo 7, apartado 1, y tendrá en cuenta la evolución del mercado y de la tecnología.

*Artículo 7*

**Modificaciones del anexo III**

1. Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73 para modificar el anexo III añadiendo o modificando casos de uso de sistemas de IA de alto riesgo cuando se cumplan las dos condiciones siguientes:

(a) los sistemas de IA están destinados a utilizarse en cualquiera de los ámbitos enumerados en los puntos 1 a 8 del anexo III;

(b) los sistemas de IA plantean un riesgo de daño para la salud y la seguridad, o un impacto adverso en los derechos fundamentales, y ese riesgo es equivalente o mayor que el riesgo de daño o de impacto adverso que plantean los sistemas de IA de alto riesgo ya mencionados en el anexo III.

2. Al evaluar, a efectos del apartado 1, si un sistema de IA plantea un riesgo de daño para la salud y la seguridad o un riesgo de impacto adverso sobre los derechos fundamentales equivalente o superior al riesgo de daño que plantean los sistemas de IA de alto riesgo ya mencionados en el anexo III, la Comisión tendrá en cuenta los siguientes criterios:

(a) la finalidad prevista del sistema de IA;

(b) la medida en que se ha utilizado o es probable que se utilice un sistema de IA;

(b bis) la naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales;

(bb) la medida en que el sistema de IA actúa de forma autónoma y la posibilidad de que un humano anule una decisión o recomendaciones que puedan provocar un daño potencial;

(c) la medida en que el uso de un sistema de IA ya ha causado daños a la salud y la seguridad, ha tenido repercusiones negativas en los derechos fundamentales o ha suscitado inquietudes importantes en relación con la probabilidad de que se produzcan tales daños o repercusiones negativas, como lo demuestran, por ejemplo, informes o alegaciones documentadas presentadas a las autoridades nacionales competentes u otros informes, según proceda;

(d) el alcance potencial de dicho daño o de dicho impacto adverso, en particular en términos de su intensidad y de su capacidad de afectar a una pluralidad de personas o de afectar desproporcionadamente a un grupo particular de personas;

(e) la medida en que las personas potencialmente perjudicadas o impactadas negativamente dependen del resultado producido con un sistema de IA, en particular porque por razones prácticas o legales no es razonablemente posible excluirse de ese resultado;

la medida en que existe un desequilibrio de poder, o las personas potencialmente perjudicadas o impactadas negativamente se encuentran en una posición vulnerable en relación con el usuario de un sistema de IA, en particular debido a su estatus, autoridad, conocimientos, circunstancias económicas o sociales, o edad;

(f) la medida en que el resultado producido por un sistema de IA es fácilmente corregible o reversible, teniendo en cuenta las soluciones técnicas disponibles para corregirlo o revertirlo; los resultados que tengan un impacto adverso sobre la salud, la seguridad o los derechos fundamentales no se considerarán fácilmente corregibles o reversibles;

(g ter) la magnitud y probabilidad del beneficio del despliegue del sistema de IA para individuos, grupos o la sociedad en general, incluidas las posibles mejoras en la seguridad de los productos;

(g) en qué medida lo prevé la legislación vigente de la Unión:

(h) medidas efectivas de reparación en relación con los riesgos que plantea un sistema de IA, con exclusión de las reclamaciones por daños y perjuicios;

(ii)medidas eficaces para prevenir o reducir sustancialmente dichos riesgos.

2 bis) La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 73 a fin de modificar la lista del anexo III suprimiendo los sistemas de IA de alto riesgo cuando se cumplan las dos condiciones siguientes:

(a) el sistema o sistemas de IA de alto riesgo de que se trate ya no plantean riesgos significativos para los derechos fundamentales, la salud o la seguridad, teniendo en cuenta los criterios enumerados en el apartado 2;

(b) la supresión no disminuye el nivel general de protección de la salud, la seguridad y los derechos fundamentales con arreglo al Derecho de la Unión.

# Capítulo 2

# REQUISITOS PARA LOS SISTEMAS DE AI DE ALTO RIESGO

*Artículo 8*

**Cumplimiento de los requisitos**

1. Los sistemas de IA de alto riesgo deberán cumplir los requisitos establecidos en el presente capítulo, teniendo en cuenta su finalidad prevista, así como el estado generalmente reconocido de la

arte de la IA y las tecnologías relacionadas con la IA. El sistema de gestión de riesgos a que se refiere el artículo 9 se tendrá en cuenta a la hora de garantizar el cumplimiento de dichos requisitos.

2 bis. Cuando un producto contenga un sistema de inteligencia artificial al que se apliquen los requisitos del presente Reglamento, así como los requisitos de la legislación de armonización de la Unión enumerados en el anexo II, sección A, los proveedores serán responsables de garantizar que su producto cumple plenamente todos los requisitos aplicables exigidos en virtud de la legislación de armonización de la Unión. 2. Al garantizar la conformidad de los sistemas de IA de alto riesgo a que se refiere el apartado 1 con los requisitos establecidos en el capítulo 2 del presente título, y con el fin de garantizar la coherencia, evitar duplicaciones y minimizar las cargas adicionales, los proveedores tendrán la opción de integrar, según proceda, los procesos necesarios de ensayo y notificación, la información y la documentación que faciliten en relación con su producto en la documentación y los procedimientos ya existentes exigidos en virtud de la legislación de armonización de la Unión enumerada en el anexo II, sección A.

*Artículo 9*

**Sistema de gestión de riesgos**

1. Se establecerá, aplicará, documentará y mantendrá un sistema de gestión de riesgos en relación con los sistemas de IA de alto riesgo.

2. El sistema de gestión de riesgos se entenderá como un proceso iterativo continuo, planificado y ejecutado a lo largo de todo el ciclo de vida de un sistema de IA de alto riesgo, que requiere una revisión y actualización periódicas y sistemáticas. Comprenderá las siguientes etapas:

(a) identificación y análisis de los riesgos conocidos y de los riesgos razonablemente previsibles que el sistema de IA de alto riesgo puede plantear para la salud, la seguridad o los derechos fundamentales cuando el sistema de IA de alto riesgo se utiliza de acuerdo con su finalidad prevista;

(b) estimación y evaluación de los riesgos que pueden surgir cuando el sistema de IA de alto riesgo se utiliza de acuerdo con su finalidad prevista y en condiciones de uso indebido razonablemente previsibles;

(c) la evaluación de otros riesgos que puedan surgir, basada en el análisis de los datos recogidos en el sistema de seguimiento poscomercialización contemplado en el artículo 61;

(d) adopción de medidas adecuadas y específicas de gestión de riesgos destinadas a hacer frente a los riesgos identificados en virtud de la letra a del presente apartado, de conformidad con lo dispuesto en los apartados siguientes.

2a. Los riesgos a que se refiere el presente apartado se referirán únicamente a aquellos que puedan mitigarse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema de IA de alto riesgo, o el suministro de información técnica adecuada.

3. Las medidas de gestión de riesgos contempladas en el apartado 2, letra d), tendrán debidamente en cuenta los efectos y la posible interacción resultantes de la aplicación combinada de los requisitos establecidos en el presente capítulo 2, con vistas a minimizar los riesgos de forma más eficaz y lograr al mismo tiempo un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos.

4. Las medidas de gestión de riesgos a que se refiere el apartado 2, letra d), serán tales que el riesgo residual pertinente asociado a cada peligro, así como el riesgo residual global de los sistemas de IA de alto riesgo, se consideren aceptables.

A la hora de determinar las medidas de gestión de riesgos más adecuadas, se garantizará lo siguiente:

(a) eliminación o reducción de los riesgos identificados y evaluados con arreglo al apartado 2, en la medida en que sea técnicamente viable, mediante un diseño y desarrollo adecuados del sistema de IA de alto riesgo;

(b) en su caso, aplicación de medidas adecuadas de mitigación y control de los riesgos que no puedan eliminarse;

(c) el suministro de la información requerida en virtud del artículo 13, a que se refiere la letra b) del apartado 2 del presente artículo, y, en su caso, la formación de los encargados del despliegue.

Con vistas a eliminar o reducir los riesgos relacionados con el uso del sistema de IA de alto riesgo, se tendrán debidamente en cuenta los conocimientos técnicos, la experiencia, la educación y la formación que cabe esperar de la persona que vaya a utilizar el sistema, así como el contexto presumible en el que vaya a utilizarse.

5. Los sistemas de IA de alto riesgo se someterán a pruebas con el fin de determinar las medidas de gestión de riesgos más adecuadas y específicas. Las pruebas garantizarán que los sistemas de IA de alto riesgo funcionan de manera coherente para los fines previstos y cumplen los requisitos establecidos en el presente capítulo.

6. Los procedimientos de ensayo podrán incluir pruebas en condiciones reales de conformidad con el artículo 54 bis.

7. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en cualquier caso, antes de la puesta en el

mercado o la puesta en servicio. Las pruebas se realizarán en función de parámetros y umbrales probabilísticos previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo.

8. Al aplicar el sistema de gestión de riesgos descrito en los apartados 1 a 6, los proveedores tendrán en cuenta si, habida cuenta de su finalidad prevista, el sistema de IA de alto riesgo puede afectar negativamente a los menores de 18 años y, en su caso, a otros grupos vulnerables de personas.

9. Para los proveedores de sistemas de IA de alto riesgo que estén sujetos a requisitos relativos a los procesos internos de gestión de riesgos en virtud de la legislación sectorial pertinente de la Unión, los aspectos descritos en los apartados 1 a 8 podrán formar parte de los procedimientos de gestión de riesgos establecidos con arreglo a dicha legislación o combinarse con ellos.

*Artículo 10*

**Datos y gobernanza de datos**

1. Los sistemas de IA de alto riesgo que hagan uso de técnicas que impliquen el entrenamiento de modelos con datos se desarrollarán sobre la base de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad contemplados en los apartados 2 a 5 siempre que se utilicen dichos conjuntos de datos.

2. Los conjuntos de datos de entrenamiento, validación y ensayo estarán sujetos a prácticas adecuadas de gobernanza y gestión de datos apropiadas para la finalidad prevista del sistema de IA. Dichas prácticas se referirán en particular a

(a) las opciones de diseño pertinentes;

(aa) los procesos de recogida de datos y el origen de los mismos y, en el caso de los datos personales, la finalidad original de la recogida de datos;

(c) operaciones pertinentes de tratamiento de preparación de datos, como anotación, etiquetado, limpieza, actualización, enriquecimiento y agregación;

(d) la formulación de hipótesis, en particular con respecto a la información que los datos deben medir y representar;

(e) una evaluación de la disponibilidad, cantidad e idoneidad de los conjuntos de datos necesarios;

(f) examen a la vista de posibles sesgos que puedan afectar a la salud y la seguridad de las personas, repercutir negativamente en los derechos fundamentales o dar lugar a discriminaciones prohibidas

en virtud del Derecho de la Unión, especialmente cuando la producción de datos influye en los insumos para futuras operaciones;

(f bis) medidas adecuadas para detectar, prevenir y mitigar los posibles sesgos detectados con arreglo a la letra f);

(g) la identificación de las lagunas o deficiencias de datos pertinentes que impidan el cumplimiento del presente Reglamento, y la forma de subsanar dichas lagunas y deficiencias.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la medida de lo posible, estarán exentos de errores y serán completos con vistas a la finalidad prevista. Deberán tener las propiedades estadísticas adecuadas, incluso, en su caso, en lo que se refiere a las personas o grupos de personas en relación con los cuales está previsto utilizar el sistema de IA de alto riesgo. Estas características de los conjuntos de datos podrán cumplirse a nivel de conjuntos de datos individuales o de una combinación de los mismos.

4. Los conjuntos de datos tendrán en cuenta, en la medida en que lo exija la finalidad prevista, las características o los elementos propios del entorno geográfico, contextual, conductual o funcional específico en el que esté previsto utilizar el sistema de IA de alto riesgo.

5. En la medida en que sea estrictamente necesario para garantizar la detección y corrección de sesgos en relación con los sistemas de IA de alto riesgo de conformidad con el párrafo segundo, letra f) y f bis), los proveedores de dichos sistemas podrán tratar excepcionalmente categorías especiales de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725, se aplicarán todas las condiciones siguientes para que se produzca dicho tratamiento:

(a) la detección y corrección de sesgos no puede realizarse eficazmente mediante el tratamiento de otros datos, incluidos los datos sintéticos o anónimos;

(b) las categorías especiales de datos personales tratados a efectos del presente apartado están sujetas a limitaciones técnicas en cuanto a la reutilización de los datos personales y a las medidas más avanzadas de seguridad y preservación de la intimidad, incluida la seudonimización;

(c) las categorías especiales de datos personales tratados a efectos del presente apartado estén sujetas a medidas que garanticen la seguridad y protección de los datos personales tratados,

sujetos a las salvaguardias adecuadas, incluidos controles estrictos y documentación del acceso, para evitar usos indebidos y garantizar que sólo las personas autorizadas tengan acceso a esos datos personales con las obligaciones de confidencialidad adecuadas;

(d) las categorías especiales de datos personales tratados a efectos del presente apartado no se transmitirán, transferirán ni serán accesibles de otro modo a terceros;

(e) las categorías especiales de datos personales tratados a efectos del presente apartado se suprimirán una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, lo que ocurra primero;

(f) los registros de actividades de tratamiento de conformidad con el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725 incluyen la justificación de por qué el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos y este objetivo no podía lograrse mediante el tratamiento de otros datos.

6. Para el desarrollo de sistemas de IA de alto riesgo que no utilicen técnicas que impliquen el entrenamiento de modelos, los apartados 2 a 5 se aplicarán únicamente a los conjuntos de datos de prueba.

*Artículo 11*

**Documentación técnica**

1. La documentación técnica de un sistema de IA de alto riesgo se elaborará antes de su comercialización o puesta en servicio y se mantendrá actualizada.

La documentación técnica se elaborará de forma que demuestre que el sistema de IA de alto riesgo cumple los requisitos establecidos en el presente capítulo y proporcione a las autoridades nacionales competentes y a los organismos notificados la información necesaria de forma clara y completa para evaluar la conformidad del sistema de IA con dichos requisitos. Contendrá, como mínimo, los elementos establecidos en el anexo IV. Las PYME, incluidas las de nueva creación, podrán facilitar los elementos de la documentación técnica especificados en el anexo IV de forma simplificada. A tal efecto, la Comisión establecerá un formulario simplificado de documentación técnica orientado a las necesidades de las pequeñas empresas y microempresas. Cuando una PYME, incluidas las de nueva creación, opte por facilitar la información requerida en el anexo IV de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán el formulario a efectos de evaluación de la conformidad.

2. Cuando se comercialice o se ponga en servicio un sistema de IA de alto riesgo relacionado con un producto al que se apliquen los actos jurídicos enumerados en la sección A del anexo II, una sola técnica

se elaborará una documentación que contenga toda la información establecida en el apartado 1, así como la información exigida en virtud de dichos actos jurídicos.

3. Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73 a fin de modificar el anexo IV cuando sea necesario para garantizar que, a la luz del progreso técnico, la documentación técnica proporcione toda la información necesaria para evaluar la conformidad del sistema con los requisitos establecidos en el presente capítulo.

*Artículo 12*

**Mantenimiento de registros**

1. Los sistemas de IA de alto riesgo deberán permitir técnicamente el registro automático de eventos ("logs") durante toda la vida útil del sistema.

2. Con el fin de garantizar un nivel de trazabilidad del funcionamiento del sistema de IA adecuado a la finalidad prevista del sistema, las capacidades de registro permitirán la grabación de eventos relevantes para:

(i) identificación de situaciones que puedan dar lugar a que el sistema de IA presente un riesgo en el sentido del apartado 1 del artículo 65 o a una modificación sustancial;

(ii) facilitar el seguimiento postcomercialización a que se refiere el artículo 61; y

(iii) supervisión del funcionamiento de los sistemas de IA de alto riesgo a que se refiere el apartado 4 del artículo 29.

4. Para los sistemas de IA de alto riesgo a que se refiere el apartado 1, letra a), del anexo III, las capacidades de registro proporcionarán, como mínimo:

(a) registro del periodo de cada uso del sistema (fecha y hora de inicio y fecha y hora de fin de cada uso);

(b) la base de datos de referencia con la que el sistema ha cotejado los datos de entrada;

(c) los datos de entrada para los que la búsqueda ha conducido a una coincidencia;

(d) la identificación de las personas físicas que participan en la verificación de los resultados, según lo dispuesto en el apartado 5 del artículo 14.

*Artículo 13*

**Transparencia y suministro de información a los usuarios**

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de forma que se garantice que su funcionamiento es lo suficientemente transparente como para permitir a los implantadores interpretar los resultados del sistema y utilizarlos adecuadamente. Se garantizará un tipo y grado de transparencia adecuados con vistas a lograr el cumplimiento de las obligaciones pertinentes del proveedor y del implantador establecidas en el capítulo 3 del presente título.

2. Los sistemas de IA de alto riesgo irán acompañados de instrucciones de uso en un formato digital adecuado o de otro tipo que incluya información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios.

3. Las instrucciones de uso contendrán como mínimo la siguiente información:

(a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado;

(b) las características, capacidades y limitaciones de rendimiento del sistema de IA de alto riesgo, incluyendo:

(i) su finalidad prevista;

(ii) el nivel de precisión, incluidas sus métricas, robustez y ciberseguridad a que se refiere el artículo 15, con respecto al cual se ha probado y validado el sistema de IA de alto riesgo y que cabe esperar, así como cualquier circunstancia conocida y previsible que pueda repercutir en ese nivel previsto de precisión, robustez y ciberseguridad;

(iii) cualquier circunstancia conocida o previsible, relacionada con el uso del sistema de IA de alto riesgo de conformidad con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales a que se refiere el artículo 9, apartado 2;

(iiia) en su caso, las capacidades y características técnicas del sistema de IA para proporcionar información que sea relevante para explicar su producción;

(iv) cuando proceda, sus prestaciones en relación con las personas o grupos de personas específicos en los que se vaya a utilizar el sistema;

cuando proceda, especificaciones de los datos de entrada, o cualquier otra información pertinente en cuanto a los conjuntos de datos de entrenamiento, validación y prueba utilizados, teniendo en cuenta la finalidad prevista del sistema de IA;

(v bis) en su caso, información que permita a los responsables de la implantación interpretar los resultados del sistema y utilizarlos adecuadamente.

(c) los cambios introducidos en el sistema de IA de alto riesgo y en sus prestaciones que hayan sido determinados previamente por el proveedor en el momento de la evaluación inicial de la conformidad, en su caso;

(d) las medidas de supervisión humana contempladas en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de los sistemas de IA por parte de quienes los despliegan;

(e) los recursos informáticos y de hardware necesarios, la vida útil prevista del sistema de IA de alto riesgo y las medidas de mantenimiento y cuidado necesarias, incluida su frecuencia, para garantizar el correcto funcionamiento de dicho sistema de IA, incluso en lo que respecta a las actualizaciones de software;

(e bis) cuando proceda, una descripción de los mecanismos incluidos en el sistema de IA que permitan a los usuarios recopilar, almacenar e interpretar adecuadamente los registros de conformidad con el artículo 12.

*Artículo 14*

**Supervisión humana**

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de tal manera, incluso con herramientas adecuadas de interfaz hombre-máquina, que puedan ser supervisados eficazmente por personas físicas durante el periodo en que el sistema de IA esté en uso.

2. La supervisión humana tendrá por objeto prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que puedan surgir cuando un sistema de IA de alto riesgo se utilice de acuerdo con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos establecidos en el presente capítulo.

3. Las medidas de supervisión serán proporcionales a los riesgos, el nivel de autonomía y el contexto de uso del sistema de IA y se garantizarán mediante uno o todos los tipos de medidas siguientes:

medidas identificadas e incorporadas, cuando sea técnicamente viable, al sistema de IA de alto riesgo por el proveedor antes de su comercialización o puesta en servicio;

(a) medidas identificadas por el proveedor antes de comercializar o poner en servicio el sistema de IA de alto riesgo y que sean adecuadas para ser aplicadas por el usuario.

4. 4. A efectos de la aplicación de los apartados 1 a 3, el sistema de IA de alto riesgo se facilitará al usuario de forma que se habilite a las personas físicas a las que se asigne la supervisión humana, según resulte adecuado y proporcionado a las circunstancias:

(a) comprender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder supervisar debidamente su funcionamiento, también con vistas a detectar y abordar anomalías, disfunciones y rendimientos inesperados;

(b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados producidos por un sistema de IA de alto riesgo ("sesgo de automatización"), en particular en el caso de los sistemas de IA de alto riesgo utilizados para proporcionar información o recomendaciones para las decisiones que deben tomar las personas físicas;

(c) interpretar correctamente los resultados del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, las herramientas y métodos de interpretación disponibles;

(d) decidir, en una situación concreta, no utilizar el sistema de IA de alto riesgo o ignorar, anular o invertir de otro modo los resultados del sistema de IA de alto riesgo;

(e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir, el sistema mediante un botón de "parada" o un procedimiento similar que permita detener el sistema en un estado seguro.

5. En el caso de los sistemas de IA de alto riesgo a que se refiere la letra a) del punto 1 del Anexo III, las medidas a que se refiere el apartado 3 deberán garantizar que, además, el responsable del despliegue no tome ninguna medida o decisión sobre la base de la identificación resultante del sistema a menos que ésta haya sido verificada y confirmada por separado por al menos dos personas físicas con la competencia, la formación y la autoridad necesarias.

El requisito de verificación por separado por parte de al menos dos personas físicas no se aplicará a los sistemas de IA de alto riesgo utilizados a efectos policiales, de migración, de control fronterizo o de asilo, en los casos en que el Derecho de la Unión o nacional considere desproporcionada la aplicación de este requisito.

*Artículo 15*

**Precisión, solidez y ciberseguridad**

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de forma que alcancen un nivel adecuado de precisión, solidez y ciberseguridad, y funcionen de forma coherente en esos aspectos a lo largo de su ciclo de vida.

1 bis. Para abordar los aspectos técnicos de cómo medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 del presente artículo y cualquier otra métrica de rendimiento pertinente, la Comisión, en cooperación con las partes interesadas y las organizaciones pertinentes, como las autoridades de metrología y evaluación comparativa, fomentará, según proceda, el desarrollo de referencias y metodologías de medición.

2. Los niveles de precisión y las métricas de precisión pertinentes de los sistemas de IA de alto riesgo se declararán en las instrucciones de uso adjuntas.

3. Los sistemas de IA de alto riesgo deberán ser lo más resistentes posible frente a los errores, fallos o incoherencias que puedan producirse en el sistema o en el entorno en el que opera el sistema, en particular debido a su interacción con personas físicas u otros sistemas. Se adoptarán medidas técnicas y organizativas a este respecto.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones técnicas de redundancia, que pueden incluir planes de respaldo o a prueba de fallos.

Los sistemas de IA de alto riesgo que sigan aprendiendo después de su comercialización o puesta en servicio se desarrollarán de tal manera que se elimine o reduzca en la medida de lo posible el riesgo de que los resultados posiblemente sesgados influyan en los datos de entrada para futuras operaciones ("bucles de retroalimentación") se aborden debidamente con medidas de mitigación adecuadas.

4. Los sistemas de IA de alto riesgo deberán ser resistentes a los intentos de terceros no autorizados de alterar su uso, resultados o rendimiento aprovechando las vulnerabilidades del sistema.

Las soluciones técnicas destinadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo deberán ser adecuadas a las circunstancias pertinentes y a los riesgos.

Las soluciones técnicas para hacer frente a las vulnerabilidades específicas de la IA incluirán, en su caso, medidas para prevenir, detectar, responder, resolver y controlar los ataques que intenten manipular el conjunto de datos de entrenamiento ("envenenamiento de datos"), o los componentes preentrenados utilizados en el entrenamiento ("envenenamiento del modelo"), las entradas diseñadas para hacer que el modelo cometa un error ("ejemplos adversos" o "evasión del modelo"), los ataques a la confidencialidad o los defectos del modelo.

# Capítulo 3

# OBLIGACIONES DE LOS PROVEEDORES E IMPLANTADORES DE SISTEMAS DE AI DE ALTO RIESGO Y OTRAS PARTES

*Artículo 16*

**Obligaciones de los proveedores de sistemas de IA de alto riesgo**

Los proveedores de sistemas de IA de alto riesgo deberán:

(a) garantizar que sus sistemas de IA de alto riesgo cumplen los requisitos establecidos en el capítulo 2 del presente título;

(a bis) indicar su nombre, su nombre comercial registrado o marca comercial registrada, la dirección en la que se les puede contactar en el sistema de IA de alto riesgo o, cuando ello no sea posible, en su envase o en la documentación que lo acompañe, según proceda;

(b) disponer de un sistema de gestión de la calidad que se ajuste a lo dispuesto en el artículo 17;

(c) conservar la documentación mencionada en el artículo 18;

(d) cuando estén bajo su control, conservar los registros generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 20;

(e) garantizar que el sistema de IA de alto riesgo se someta al correspondiente procedimiento de evaluación de la conformidad a que se refiere el artículo 43, antes de su comercialización o puesta en servicio;

(e bis) redactar una declaración UE de conformidad con arreglo al artículo 48;

(e ter) colocar el marcado CE en el sistema de IA de alto riesgo para indicar su conformidad con el presente Reglamento, de conformidad con el artículo 49;

(f) cumplir las obligaciones de registro contempladas en el apartado 1 del artículo 51;

(g) adoptar las medidas correctoras necesarias y facilitar la información exigida en el artículo 21;

(j) previa solicitud motivada de una autoridad nacional competente, demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título;

(ja) garantizar que el sistema de IA de alto riesgo cumple los requisitos de accesibilidad, de conformidad con la Directiva 2019/882 sobre los requisitos de accesibilidad de productos y servicios y la Directiva 2016/2102 sobre la accesibilidad de los sitios web y las aplicaciones móviles de los organismos del sector público.

*Artículo 17*

**Sistema de gestión de la calidad**

1. Los proveedores de sistemas de IA de alto riesgo implantarán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema estará documentado de manera sistemática y ordenada en forma de políticas, procedimientos e instrucciones escritas, e incluirá al menos los siguientes aspectos:

(a) una estrategia de cumplimiento de la normativa, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y los procedimientos de gestión de las modificaciones del sistema de IA de alto riesgo;

(b) técnicas, procedimientos y acciones sistemáticas que deben utilizarse para el diseño, el control del diseño y la verificación del diseño del sistema de IA de alto riesgo;

(c) técnicas, procedimientos y acciones sistemáticas que se utilizarán para el desarrollo, el control de calidad y la garantía de calidad del sistema de IA de alto riesgo;

(d) los procedimientos de examen, prueba y validación que deben llevarse a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, y la frecuencia con que deben realizarse;

(e) las especificaciones técnicas, incluidas las normas, que deben aplicarse y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad o no cubran todos los requisitos pertinentes establecidos en el capítulo II del presente título, los medios que deben utilizarse para garantizar que el sistema de IA de alto riesgo cumple dichos requisitos;

(f) los sistemas y procedimientos de gestión de datos, incluida la adquisición de datos, la recogida de datos, el análisis de datos, el etiquetado de datos, el almacenamiento de datos, el filtrado de datos, la extracción de datos, la agregación de datos, la conservación de datos y cualquier otra operación relativa a los datos que se realice antes y a efectos de la comercialización o puesta en servicio de sistemas de IA de alto riesgo;

(g) el sistema de gestión de riesgos a que se refiere el artículo 9;

la creación, aplicación y mantenimiento de un sistema de seguimiento postcomercialización, de conformidad con el artículo 61;

(h) procedimientos relacionados con la notificación de un incidente grave de conformidad con el artículo 62;

(i) la gestión de la comunicación con las autoridades nacionales competentes, otras autoridades pertinentes, incluidas las que facilitan o apoyan el acceso a los datos, organismos notificados, otros operadores, clientes u otras partes interesadas;

(j) sistemas y procedimientos de registro de toda la documentación e información pertinentes;

(k) gestión de los recursos, incluidas las medidas relacionadas con la seguridad del suministro;

(l) un marco de rendición de cuentas que establezca las responsabilidades de la dirección y del resto del personal en relación con todos los aspectos enumerados en este apartado.

2. La aplicación de los aspectos contemplados en el apartado 1 será proporcional al tamaño de la organización del proveedor. En cualquier caso, los proveedores respetarán el grado de rigor y el nivel de protección necesarios para garantizar la conformidad de sus sistemas de IA con el presente Reglamento.

2 bis. Para los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a sistemas de gestión de la calidad o a su función equivalente en virtud de la legislación sectorial pertinente de la Unión, los aspectos descritos en el apartado 1 podrán formar parte de los sistemas de gestión de la calidad con arreglo a dicha legislación.

3. Para los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación de la Unión en materia de servicios financieros, la obligación de establecer un sistema de gestión de la calidad, con excepción de lo dispuesto en el apartado 1, letras g), h) e i), se considerará cumplida mediante el cumplimiento de las normas sobre disposiciones o procesos de gobernanza interna con arreglo a la legislación de la Unión en materia de servicios financieros pertinente. En ese contexto, se tendrán en cuenta las normas armonizadas a que se refiere el artículo 40 del presente Reglamento.

*Artículo 18*

**Conservación de la documentación**

1. El proveedor mantendrá a disposición de las autoridades nacionales competentes el sistema de IA durante un periodo que finalizará diez años después de su comercialización o puesta en servicio:

la documentación técnica contemplada en el artículo 11;

(a) la documentación relativa al sistema de gestión de la calidad a que se refiere el artículo 17;

(b) la documentación relativa a las modificaciones aprobadas por los organismos notificados, en su caso;

(c) las decisiones y otros documentos emitidos por los organismos notificados, en su caso;

(d) la declaración UE de conformidad contemplada en el artículo 48.

1 bis. Cada Estado miembro determinará las condiciones en las que la documentación a que se refiere el apartado 1 permanecerá a disposición de las autoridades nacionales competentes durante el período indicado en dicho apartado para los casos en que un prestador o su representante autorizado establecido en su territorio quiebre o cese su actividad antes de que finalice dicho período.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación sobre servicios financieros de la Unión mantendrán la documentación técnica como parte de la documentación conservada con arreglo a la legislación pertinente sobre servicios financieros de la Unión.

*Artículo 20*

**Registros generados automáticamente**

1. Los proveedores de sistemas de IA de alto riesgo conservarán los registros a que se refiere el artículo 12, apartado 1, generados automáticamente por sus sistemas de IA de alto riesgo, en la medida en que dichos registros estén bajo su control. Sin perjuicio del Derecho de la Unión o nacional aplicable, los registros se conservarán durante un período adecuado a la finalidad prevista del sistema de IA de alto riesgo, de al menos 6 meses, salvo disposición en contrario del Derecho de la Unión o nacional aplicable, en particular del Derecho de la Unión en materia de protección de datos personales.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos con arreglo a la legislación de la Unión en materia de servicios financieros conservarán los registros generados automáticamente por sus sistemas de IA de alto riesgo como parte de la documentación conservada con arreglo a la legislación pertinente en materia de servicios financieros.

*Artículo 21*

**Acciones correctoras y deber de información**

1. Los proveedores de sistemas de IA de alto riesgo que consideren o tengan motivos para considerar que un sistema de IA de alto riesgo que han introducido en el mercado o puesto en servicio no es conforme con el presente Reglamento adoptarán inmediatamente las medidas correctoras necesarias para hacerlo conforme, retirarlo del mercado, inutilizarlo o recuperarlo, según proceda. Informarán de ello a los distribuidores del sistema de IA de alto riesgo en cuestión y, en su caso, a los responsables del despliegue, al representante autorizado y a los importadores.

Cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, y el proveedor tenga conocimiento de dicho riesgo, investigará inmediatamente las causas, en colaboración con el implantador notificante, en su caso, e informará a las autoridades de vigilancia del mercado de los Estados miembros en los que haya puesto a disposición el sistema de IA de alto riesgo y, en su caso, al organismo notificado que haya expedido un certificado para el sistema de IA de alto riesgo de conformidad con el artículo 44, en particular, de la naturaleza del incumplimiento y de cualquier medida correctora pertinente que se haya adoptado.

*Artículo 23*

**Cooperación con las autoridades competentes**

1. Los proveedores de sistemas de IA de alto riesgo, previa solicitud motivada de una autoridad competente, facilitarán a dicha autoridad toda la información y documentación necesarias para demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, en una lengua fácilmente comprensible para la autoridad en una lengua oficial de la Unión determinada por el Estado miembro de que se trate.

1 bis. Previa solicitud motivada de una autoridad nacional competente, los proveedores darán también a la autoridad nacional competente solicitante, según proceda, acceso a los registros a que se refiere el artículo 12, apartado 1, generados automáticamente por el sistema de IA de alto riesgo, en la medida en que dichos registros estén bajo su control.

1 ter. Toda información obtenida por una autoridad nacional competente en virtud de lo dispuesto en el presente artículo se tratará respetando las obligaciones de confidencialidad establecidas en el artículo 70.

*Artículo 25*

**Representantes autorizados**

1. Antes de comercializar sus sistemas en el mercado de la Unión, los proveedores establecidos fuera de la Unión designarán, mediante mandato escrito, a un representante autorizado establecido en la Unión.

1 ter.El prestador permitirá a su representante autorizado desempeñar las funciones que le asigna el presente Reglamento.

2. El representante autorizado realizará las tareas especificadas en el mandato recibido del proveedor. Facilitará una copia del mandato a las autoridades de vigilancia del mercado que lo soliciten, en una de las lenguas oficiales de la institución de la Unión determinada por la autoridad nacional competente. A efectos del presente Reglamento, el mandato facultará al representante autorizado para realizar las siguientes tareas

(-a) comprobar que se han elaborado la declaración UE de conformidad y la documentación técnica y que el proveedor ha llevado a cabo un procedimiento adecuado de evaluación de la conformidad;

(a) mantener a disposición de las autoridades nacionales competentes y de las autoridades nacionales a que se refiere el artículo 63, apartado 7, durante un período que finalizará diez años después de la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, los datos de contacto del proveedor que haya designado al representante autorizado, una copia de la declaración UE de conformidad, la documentación técnica y, si procede, el certificado expedido por el organismo notificado;

(b) facilitará a una autoridad nacional competente, previa solicitud motivada, toda la información y documentación, incluida la conservada con arreglo a la letra a), necesaria para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, incluido el acceso a los registros a que se refiere el artículo 12, apartado 1, generados automáticamente por el sistema de IA de alto riesgo en la medida en que dichos registros estén bajo el control del proveedor;

(c) cooperar con las autoridades competentes, previa solicitud motivada, en cualquier acción que éstas emprendan en relación con el sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que plantea dicho sistema;

(c bis) en su caso, cumplir las obligaciones de registro contempladas en el artículo 51, apartado 1, o, si el registro lo efectúa el propio prestador, garantizar que la información contemplada en el [punto 3] del anexo VIII es correcta.

El mandato facultará al representante autorizado para que las autoridades competentes se dirijan a él, además de al prestador o en su lugar, para todas las cuestiones relacionadas con el cumplimiento del presente Reglamento.

2 ter. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor actúa de forma contraria a las obligaciones que le incumben en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la autoridad de vigilancia del mercado del Estado miembro en el que esté establecido, así como, en su caso, al organismo notificado pertinente, de la terminación del mandato y de los motivos de la misma.

*Artículo 26*

**Obligaciones de los importadores**

1. Antes de comercializar un sistema de IA de alto riesgo, los importadores de dicho sistema se asegurarán de que éste es conforme con el presente Reglamento verificando que:

(a) el proveedor de dicho sistema de IA haya llevado a cabo el correspondiente procedimiento de evaluación de la conformidad a que se refiere el artículo 43;

(b) el proveedor haya elaborado la documentación técnica de conformidad con el artículo 11 y el anexo IV;

(c) el sistema lleva el marcado CE de conformidad exigido y va acompañado de la declaración UE de conformidad y de las instrucciones de uso;

(c bis) el prestador haya designado a un representante autorizado de conformidad con el apartado 1 del artículo 25.

2. Cuando un importador tenga motivos suficientes para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, o está falsificado, o va acompañado de documentación falsificada, no introducirá dicho sistema en el mercado hasta que sea conforme. Cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, el importador informará de ello al proveedor del sistema de IA, a los representantes autorizados y a las autoridades de vigilancia del mercado.

Los importadores indicarán su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto en el sistema de IA de alto riesgo y en su embalaje o en la documentación que lo acompañe, cuando proceda.

3. 1. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán de que, en su caso, las condiciones de almacenamiento o transporte no comprometen el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título.

4a. Los importadores conservarán, durante un período de diez años después de la introducción en el mercado o la puesta en servicio del sistema de IA, una copia del certificado expedido por el organismo notificado, en su caso, de las instrucciones de uso y de la declaración UE de conformidad.

4. Los importadores facilitarán a las autoridades nacionales competentes, previa solicitud motivada, toda la información y documentación necesarias, incluida la conservada con arreglo al apartado 4 bis, para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, en una lengua fácilmente comprensible para ellas. A tal fin, velarán asimismo por que la documentación técnica pueda ponerse a disposición de dichas autoridades.

5 bis. Los importadores cooperarán con las autoridades nacionales competentes en cualquier acción que éstas emprendan, en particular para reducir y mitigar los riesgos que plantea el sistema de IA de alto riesgo.

*Artículo 27*

**Obligaciones de los distribuidores**

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores comprobarán que el sistema de IA de alto riesgo lleva el marcado CE de conformidad requerido, que va acompañado de una copia de la declaración UE de conformidad y de las instrucciones de uso, y que el proveedor y el importador del sistema, según proceda, han cumplido sus obligaciones establecidas en el artículo 16, letras aa) y b), y en el artículo 26, apartado 3, respectivamente.

2. Cuando un distribuidor considere o tenga motivos para considerar, sobre la base de la información que obra en su poder, que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en el capítulo 2 del presente título, no lo comercializará hasta que dicho sistema sea conforme con dichos requisitos. Además, cuando el sistema presente un riesgo en el sentido del artículo 65, apartado 1, el distribuidor informará de ello al proveedor o al importador del sistema, según proceda.

1. Mientras sean responsables de un sistema de IA de alto riesgo, los distribuidores se asegurarán de que, en su caso, las condiciones de almacenamiento o transporte no comprometan el cumplimiento por parte del sistema de los requisitos establecidos en el capítulo 2 del presente título.

3. El distribuidor que considere o tenga motivos para considerar, sobre la base de la información que obra en su poder, que un sistema de IA de alto riesgo que ha comercializado no es conforme con los requisitos establecidos en el capítulo 2 del presente título, adoptará las medidas correctoras necesarias para que el sistema sea conforme con dichos requisitos, retirarlo del mercado o recuperarlo, o se asegurará de que el proveedor, el importador o cualquier operador pertinente, según proceda, adopte esas medidas correctoras. Cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, el distribuidor informará inmediatamente de ello al proveedor o importador del sistema y a las autoridades nacionales competentes de los Estados miembros en los que haya comercializado el producto, facilitando detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

4. Previa solicitud motivada de una autoridad nacional competente, los distribuidores del sistema de IA de alto riesgo facilitarán a dicha autoridad toda la información y documentación relativas a sus actividades descritas en los apartados 1 a 4 necesarias para demostrar la conformidad de un sistema de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título.

5 bis. Los distribuidores cooperarán con las autoridades nacionales competentes en cualquier acción que éstas emprendan en relación con un sistema de IA del que sean distribuidores, en particular para reducir o mitigar el riesgo que plantea el sistema de IA de alto riesgo.

*Artículo 28*

**Responsabilidades a lo largo de la cadena de valor de la IA**

1. Cualquier distribuidor, importador, implantador u otro tercero será considerado proveedor de un sistema de IA de alto riesgo a efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor con arreglo al artículo 16, en cualquiera de las siguientes circunstancias:

(a) ponen su nombre o marca comercial en un sistema de IA de alto riesgo ya comercializado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignen de otro modo;

(b) introducen una modificación sustancial en un sistema de IA de alto riesgo que ya ha sido comercializado o que ya ha sido puesto en servicio y de forma que siga siendo un sistema de IA de alto riesgo de conformidad con el artículo 6;

(b bis) modifiquen la finalidad prevista de un sistema de IA, incluido un sistema de IA de propósito general, que no haya sido clasificado como de alto riesgo y que ya haya sido comercializado o puesto en servicio de tal manera que el sistema de IA se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

2. Cuando se den las circunstancias contempladas en el apartado 1, letras a) a b bis), el proveedor que inicialmente comercializó o puso en servicio el sistema de IA dejará de ser considerado proveedor de ese sistema de IA específico a efectos del presente Reglamento. Este antiguo proveedor cooperará estrechamente y facilitará la información necesaria y proporcionará el acceso técnico y demás asistencia que razonablemente quepa esperar y que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que se refiere al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo. El presente apartado no se aplicará en los casos en que el antiguo proveedor haya excluido expresamente el paso de su sistema a un sistema de alto riesgo y, por tanto, la obligación de entregar la documentación.

2 bis. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos a los que se apliquen los actos jurídicos enumerados en la sección A del anexo II, el fabricante de dichos productos se considerará el proveedor del sistema de IA de alto riesgo y estará sujeto a las obligaciones previstas en el artículo 16 en cualquiera de los supuestos siguientes:

(i) el sistema de IA de alto riesgo se comercializa junto con el producto bajo el nombre o la marca del fabricante del producto;

(ii) el sistema de IA de alto riesgo se pone en servicio con el nombre o la marca del fabricante del producto después de que éste se haya comercializado.

2 ter. El proveedor de un sistema de IA de alto riesgo y el tercero que suministre un sistema de IA, herramientas, servicios, componentes o procesos que se utilicen o integren en un sistema de IA de alto riesgo especificarán, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y demás asistencia necesarios sobre la base del estado de la técnica generalmente reconocido, a fin de que el proveedor del sistema de IA de alto riesgo pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento. Esta obligación no se aplicará a los terceros que pongan a disposición del público herramientas, servicios, procesos o componentes de IA distintos de los modelos de IA de uso general con arreglo a una licencia libre y abierta.

La Oficina de IA podrá desarrollar y recomendar modelos voluntarios de condiciones contractuales entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en sistemas de IA de alto riesgo. Al desarrollar

En la elaboración de los modelos de cláusulas contractuales voluntarias, la Oficina de AI tendrá en cuenta los posibles requisitos contractuales aplicables en sectores o casos empresariales específicos. Los modelos de cláusulas contractuales se publicarán y estarán disponibles gratuitamente en un formato electrónico de fácil uso.

2b. Los apartados 2 y 2a se entienden sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

*Artículo 29*

**Obligaciones de los implantadores de sistemas de IA de alto riesgo**

1. Los responsables del despliegue de sistemas de IA de alto riesgo adoptarán las medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas de conformidad con las instrucciones de uso que acompañan a los sistemas, con arreglo a los apartados 2 y 5 del presente artículo.

1a. En la medida en que los responsables del despliegue ejerzan control sobre el sistema de IA de alto riesgo, velarán por que las personas físicas asignadas para garantizar la supervisión humana de los sistemas de IA de alto riesgo tengan la competencia, formación y autoridad necesarias, así como el apoyo necesario.

2. Las obligaciones de los apartados 1 y 1 bis, se entienden sin perjuicio de otras obligaciones del desplegador en virtud de la legislación de la Unión o nacional y de la discrecionalidad del desplegador para organizar sus propios recursos y actividades con el fin de aplicar las medidas de supervisión humana indicadas por el proveedor.

3. Sin perjuicio de lo dispuesto en los apartados 1 y 1 bis, en la medida en que el implantador ejerza control sobre los datos de entrada, garantizará que dichos datos sean pertinentes y suficientemente representativos a la vista de la finalidad prevista del sistema de IA de alto riesgo.

4. Los responsables del despliegue supervisarán el funcionamiento del sistema de IA de alto riesgo sobre la base de las instrucciones de uso y, cuando proceda, informarán a los proveedores de conformidad con el artículo 61. Cuando tengan motivos para considerar que el uso conforme a las instrucciones de uso puede dar lugar a que el sistema de IA presente un riesgo en el sentido del artículo 65, apartado 1, informarán sin demora injustificada al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente y suspenderán el uso del sistema. Asimismo, informarán inmediatamente primero al proveedor y después al importador o distribuidor y a las autoridades de vigilancia del mercado pertinentes cuando hayan detectado cualquier incidente grave. Si el implantador no puede ponerse en contacto con el proveedor, se aplicará mutatis mutandis el artículo 62. Esta obligación

no abarcará los datos operativos sensibles de los implantadores de sistemas de IA que sean autoridades policiales.

En el caso de los implementadores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación sobre servicios financieros de la Unión, la obligación de supervisión establecida en el párrafo primero se considerará cumplida mediante el cumplimiento de las normas sobre disposiciones, procesos y mecanismos de gobernanza interna en virtud de la legislación sobre servicios financieros pertinente.

5. Los implantadores de sistemas de IA de alto riesgo conservarán los registros generados automáticamente por dicho sistema de IA de alto riesgo, en la medida en que dichos registros estén bajo su control, durante un período adecuado a la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo disposición en contrario del Derecho de la Unión o nacional aplicable, en particular del Derecho de la Unión en materia de protección de datos personales.

Los Desplegadores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación sobre servicios financieros de la Unión mantendrán los registros como parte de la documentación conservada de conformidad con la legislación pertinente sobre servicios financieros de la Unión.

(a) Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empresarios informarán a los representantes de los trabajadores y a los trabajadores afectados de que van a estar sometidos al sistema. Esta información se facilitará, en su caso, de conformidad con las normas y procedimientos establecidos en el Derecho y las prácticas de la Unión y nacionales en materia de información de los trabajadores y sus representantes.

(b) Los implantadores de sistemas de IA de alto riesgo que sean autoridades públicas o instituciones, órganos y organismos de la Unión cumplirán las obligaciones de registro a que se refiere el artículo 51. Cuando comprueben que el sistema que tienen previsto utilizar no ha sido registrado en la base de datos de la UE a que se refiere el artículo 60, no utilizarán dicho sistema e informarán de ello al proveedor o al distribuidor.

6. Cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo utilizarán la información facilitada en virtud del artículo 13 para cumplir con su obligación de realizar una evaluación de impacto relativa a la protección de datos con arreglo al artículo 35 del Reglamento (UE) 2016/679 o al artículo 27 de la Directiva (UE) 2016/680.

6a. Sin perjuicio de lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación para el registro selectivo de una persona condenada o sospechosa de haber cometido una infracción penal, el implantador de un sistema de IA para la identificación biométrica a distancia solicitará un

autorización, previa, o sin demora indebida y a más tardar en 48 horas, de una autoridad judicial o de una autoridad administrativa cuya decisión sea vinculante y susceptible de control jurisdiccional, para la utilización del sistema, excepto cuando el sistema se utilice para la identificación inicial de un posible sospechoso basada en hechos objetivos y verificables directamente relacionados con el delito. Cada uso se limitará a lo estrictamente necesario para la investigación de una infracción penal específica.

En caso de que se deniegue la autorización solicitada prevista en el párrafo primero del presente apartado, se interrumpirá con efecto inmediato la utilización del sistema de identificación biométrica a distancia postal vinculado a dicha autorización y se suprimirán los datos personales vinculados a la utilización del sistema para el que se solicitó la autorización.

En cualquier caso, dicho sistema de IA para la identificación biométrica a distancia no se utilizará con fines policiales de forma no selectiva, sin relación alguna con un delito, un procedimiento penal, una amenaza real y actual o real y previsible de delito o la búsqueda de una persona desaparecida concreta.

Se garantizará que las autoridades policiales no puedan tomar ninguna decisión que produzca un efecto jurídico adverso sobre una persona basándose únicamente en los resultados de estos sistemas de identificación biométrica a distancia.

El presente apartado se entiende sin perjuicio de lo dispuesto en el artículo 10 de la Directiva (UE) 2016/680 y en el artículo 9 del RGPD para el tratamiento de datos biométricos.

Independientemente de la finalidad o de quien los despliegue, cada uso de estos sistemas se documentará en el expediente policial pertinente y se pondrá a disposición de la autoridad de vigilancia del mercado pertinente y de la autoridad nacional de protección de datos previa solicitud, excluida la divulgación de datos operativos sensibles relacionados con la aplicación de la ley. El presente párrafo se entenderá sin perjuicio de las facultades conferidas por la Directiva 2016/680 a las autoridades de supervisión.

Además, los responsables del despliegue presentarán informes anuales a las autoridades pertinentes de vigilancia del mercado y de protección de datos nacionales sobre los usos de los sistemas de identificación biométrica a distancia, excluyendo la divulgación de datos operativos sensibles relacionados con la aplicación de la ley. Los informes podrán agregarse para cubrir varios despliegues en una misma operación.

Los Estados miembros podrán introducir, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica a distancia.

6 ter. Sin perjuicio de lo dispuesto en el artículo 52, los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas informarán al

personas físicas que están sujetas al uso del sistema de IA de alto riesgo. Para los sistemas de IA de alto riesgo utilizados con fines policiales se aplicará el artículo 13 de la Directiva 2016/680.

6 quáter. Los responsables del despliegue cooperarán con las autoridades nacionales competentes en cualquier acción que dichas autoridades emprendan en relación con el sistema de alto riesgo con el fin de aplicar el presente Reglamento.

*Artículo 29 bis*

**Evaluación del impacto sobre los derechos fundamentales de los sistemas de IA de alto riesgo**

1. Antes de desplegar un sistema de IA de alto riesgo, tal como se define en el apartado 2 del artículo 6, con excepción de los sistemas de IA destinados a ser utilizados en el ámbito enumerado en el punto 2 del anexo III, los desplegadores que sean organismos de Derecho público u operadores privados que presten servicios públicos y los operadores que desplieguen sistemas de alto riesgo a que se refieren las letras b) y c bis) del punto 5 del anexo III realizarán una evaluación del impacto sobre los derechos fundamentales que la utilización del sistema pueda producir.

Para ello, los responsables del despliegue realizarán una evaluación consistente en:

(a) una descripción de los procesos del implantador en los que se utilizará el sistema de IA de alto riesgo de acuerdo con su finalidad prevista;

(b) una descripción del periodo de tiempo y la frecuencia con que se prevé utilizar cada sistema de IA de alto riesgo;

(c) las categorías de personas físicas y grupos que puedan verse afectados por su uso en el contexto específico;

(d) los riesgos específicos de daños que puedan afectar a las categorías de personas o grupos de personas identificados con arreglo a la letra c), teniendo en cuenta la información facilitada por el prestador con arreglo al artículo 13;

(e) una descripción de la aplicación de las medidas de supervisión humana, de acuerdo con las instrucciones de uso;

(f) las medidas que deben adoptarse en caso de materialización de estos riesgos, incluidas sus disposiciones en materia de gobernanza interna y mecanismos de denuncia.

2. La obligación establecida en el apartado 1 se aplica al primer uso del sistema de IA de alto riesgo. El implantador podrá, en casos similares, basarse en evaluaciones de impacto sobre los derechos fundamentales realizadas previamente o en evaluaciones de impacto existentes llevadas a cabo por el proveedor. Si, durante la utilización del sistema de IA de alto riesgo, el implantador considera que alguno de los factores enumerados en el apartado 1

cambian son o ya no están actualizados, el implantador tomará las medidas necesarias para actualizar la información.

3. Una vez realizada la evaluación de impacto, el responsable del despliegue notificará a la autoridad de vigilancia del mercado los resultados de la evaluación, presentando la plantilla cumplimentada a que se refiere el apartado 5 como parte de la notificación. En el caso contemplado en el artículo 47, apartado 1, los responsables del despliegue podrán quedar exentos de estas obligaciones.

4. Si alguna de las obligaciones establecidas en el presente artículo ya se cumple mediante la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 se realizará conjuntamente con dicha evaluación de impacto relativa a la protección de datos.

5. La Oficina de AI elaborará un modelo de cuestionario, incluso mediante una herramienta automatizada, para facilitar a los responsables del despliegue el cumplimiento de las obligaciones del presente artículo de forma simplificada.

# Capítulo 4

# AUTORIDADES NOTIFICANTES Y ORGANISMOS NOTIFICADOS

*Artículo 30*

**Notificación a las autoridades**

1. 1. Cada Estado miembro designará o establecerá al menos una autoridad notificante responsable de establecer y aplicar los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad y de su supervisión. Estos procedimientos se desarrollarán en cooperación con las autoridades notificantes de todos los Estados miembros.

2. Los Estados miembros podrán decidir que la evaluación y el seguimiento a que se refiere el apartado 1 sean realizados por un organismo nacional de acreditación en el sentido del Reglamento (CE) nº 765/2008 y de conformidad con el mismo.

3. Las autoridades notificantes se establecerán, organizarán y gestionarán de manera que no exista ningún conflicto de intereses con los organismos de evaluación de la conformidad y se preserve la objetividad e imparcialidad de sus actividades.

Las autoridades notificantes se organizarán de forma que las decisiones relativas a la notificación de los organismos de evaluación de la conformidad sean adoptadas por personas competentes distintas de las que llevaron a cabo la evaluación de dichos organismos.

4. Las autoridades notificantes no ofrecerán ni ejercerán ninguna actividad que efectúen los organismos de evaluación de la conformidad, ni servicios de consultoría de carácter comercial o competitivo.

5. Las autoridades notificantes salvaguardarán la confidencialidad de la información que obtengan con arreglo al artículo 70.

6. Las autoridades notificantes dispondrán de un número adecuado de personal competente para el correcto desempeño de sus funciones. El personal competente poseerá los conocimientos especializados necesarios, en su caso, para su función, en ámbitos como las tecnologías de la información, la inteligencia artificial y el Derecho, incluida la supervisión de los derechos fundamentales.

*Artículo 31*

**Solicitud de notificación de un organismo de evaluación de la conformidad**

1. Los organismos de evaluación de la conformidad presentarán una solicitud de notificación a la autoridad notificante del Estado miembro en el que estén establecidos.

2. La solicitud de notificación irá acompañada de una descripción de las actividades de evaluación de la conformidad, del módulo o módulos de evaluación de la conformidad y de los tipos de sistemas de IA para los que el organismo de evaluación de la conformidad se considere competente, así como de un certificado de acreditación, si lo hay, expedido por un organismo nacional de acreditación, que declare que el organismo de evaluación de la conformidad cumple los requisitos establecidos en el artículo

33. Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante con arreglo a cualquier otra legislación de armonización de la Unión.

3. 3. Cuando el organismo de evaluación de la conformidad en cuestión no pueda facilitar un certificado de acreditación, entregará a la autoridad notificante todas las pruebas documentales necesarias para la verificación, el reconocimiento y el seguimiento regular del cumplimiento de los requisitos establecidos en el artículo 33. En el caso de los organismos notificados que hayan sido designados con arreglo a cualquier otra legislación de armonización de la Unión, todos los documentos y certificados relacionados con esas designaciones podrán utilizarse para apoyar su procedimiento de designación con arreglo al presente Reglamento, según proceda. 4. El organismo notificado actualizará la documentación a que se refieren los apartados 2 y 3 siempre que se produzcan cambios pertinentes, a fin de que la autoridad pueda

responsable de que los organismos notificados supervisen y verifiquen el cumplimiento continuo de todos los requisitos establecidos en el artículo 33.

*Artículo 32*

**Procedimiento de notificación**

1. Las autoridades notificantes sólo podrán notificar organismos de evaluación de la conformidad que satisfagan los requisitos establecidos en el artículo 33.

2. 2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros, por medio de la herramienta de notificación electrónica desarrollada y gestionada por la Comisión, cada organismo de evaluación de la conformidad a que se refiere el apartado 1.

3. 3. La notificación a que se refiere el apartado 2 incluirá información pormenorizada de las actividades de evaluación de la conformidad, el módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA de que se trate, así como la correspondiente certificación de competencia. 4. Cuando una notificación no se base en un certificado de acreditación como el mencionado en el apartado 2 del artículo 31, la autoridad notificante facilitará a la Comisión y a los demás Estados miembros pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones adoptadas para garantizar que se supervisará periódicamente a dicho organismo y que éste seguirá cumpliendo los requisitos establecidos en el artículo 33.

4. El organismo de evaluación de la conformidad en cuestión sólo podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no han formulado ninguna objeción en el plazo de dos semanas a partir de la notificación por parte de una autoridad notificante, cuando incluya un certificado de acreditación con arreglo al artículo 31, apartado 2, o de dos meses a partir de la notificación por parte de la autoridad notificante, cuando incluya las pruebas documentales con arreglo al artículo 31, apartado 3.

4 bis. En caso de que se planteen objeciones, la Comisión consultará sin demora a los Estados miembros pertinentes y al organismo de evaluación de la conformidad. En vista de ello, la Comisión decidirá si la autorización está justificada o no. La Comisión dirigirá su decisión al Estado miembro afectado y al organismo de evaluación de la conformidad pertinente.

*Artículo 33*

**Requisitos relativos a los organismos notificados**

1. Los organismos notificados deberán estar constituidos con arreglo al Derecho nacional de un Estado miembro y tener personalidad jurídica.

2. Los organismos notificados deberán cumplir los requisitos de organización, gestión de la calidad, recursos y procesos necesarios para el desempeño de sus funciones, así como los requisitos de ciberseguridad adecuados.

3. La estructura organizativa, la asignación de responsabilidades, las líneas jerárquicas y el funcionamiento de los organismos notificados deberán ser tales que garanticen la confianza en el rendimiento y en los resultados de las actividades de evaluación de la conformidad realizadas por los organismos notificados.

4. Los organismos notificados serán independientes del proveedor de un sistema de IA de alto riesgo en relación con el cual realicen actividades de evaluación de la conformidad. Los organismos notificados también serán independientes de cualquier otro agente que tenga un interés económico en el sistema de IA de alto riesgo evaluado, así como de cualquier competidor del proveedor. Esto no impedirá el uso de los sistemas de IA evaluados que sean necesarios para las operaciones del organismo de evaluación de la conformidad ni el uso de dichos sistemas para fines personales.

4 bis. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, el desarrollo, la comercialización o el uso de sistemas de IA de alto riesgo, ni representarán a las partes que participan en estas actividades. No realizarán ninguna actividad que pueda entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que hayan sido notificados. Esto se aplicará en particular a los servicios de consultoría.

5. Los organismos notificados se organizarán y funcionarán de manera que se garantice la independencia, objetividad e imparcialidad de sus actividades. Los organismos notificados documentarán y aplicarán una estructura y procedimientos para salvaguardar la imparcialidad y promover y aplicar los principios de imparcialidad en toda su organización, personal y actividades de evaluación.

6. Los organismos notificados dispondrán de procedimientos documentados que garanticen que su personal, comités, filiales, subcontratistas y cualquier organismo asociado o personal de organismos externos respetan la confidencialidad de la información con arreglo al artículo 70 que obre en su poder durante la realización de las actividades de evaluación de la conformidad, salvo cuando la legislación exija su divulgación. El personal de los organismos notificados estará obligado a

observar el secreto profesional con respecto a toda la información obtenida en el desempeño de sus funciones en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que se lleven a cabo sus actividades.

7. Los organismos notificados dispondrán de procedimientos para la realización de actividades que tengan debidamente en cuenta el tamaño de la empresa, el sector en el que opera, su estructura y el grado de complejidad del sistema de IA en cuestión.

8. Los organismos notificados suscribirán un seguro de responsabilidad civil apropiado para sus actividades de evaluación de la conformidad, a menos que la responsabilidad sea asumida por el Estado miembro en el que estén establecidos con arreglo al Derecho nacional o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

9. Los organismos notificados deberán ser capaces de desempeñar todas las tareas que les incumban en virtud del presente Reglamento con el máximo nivel de integridad profesional y con la competencia exigida en el ámbito específico, tanto si dichas tareas son realizadas por los propios organismos notificados como si se realizan en su nombre y bajo su responsabilidad.

10. Los organismos notificados dispondrán de competencias internas suficientes para poder evaluar eficazmente las tareas realizadas por terceros en su nombre. El organismo notificado dispondrá permanentemente de suficiente personal administrativo, técnico, jurídico y científico que posea experiencia y conocimientos relacionados con los tipos pertinentes de sistemas de inteligencia artificial, datos e informática de datos y con los requisitos establecidos en el capítulo 2 del presente título.

11. Los organismos notificados participarán en las actividades de coordinación a que se refiere el artículo 38. Asimismo, participarán directamente o estarán representados en los organismos europeos de normalización, o se asegurarán de que conocen y están al día de las normas pertinentes.

*Artículo 33 bis*

**Presunción de conformidad con los requisitos relativos a los organismos notificados**

Si un organismo de evaluación de la conformidad demuestra que cumple los criterios establecidos en las normas armonizadas pertinentes o partes de las mismas cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea, se presumirá que cumple los requisitos establecidos en el artículo 33 en la medida en que las normas armonizadas aplicables cubran esos requisitos.

*Artículo 34*

**Filiales y subcontratación de organismos notificados**

1. 1. Cuando un organismo notificado subcontrate tareas específicas relacionadas con la evaluación de la conformidad o recurra a una filial, se asegurará de que el subcontratista o la filial cumplen los requisitos establecidos en el artículo 33 e informará a la autoridad notificante en consecuencia.

2. Los organismos notificados asumirán la plena responsabilidad de las tareas realizadas por subcontratistas o filiales, dondequiera que estén establecidos.

3. Las actividades sólo podrán ser subcontratadas o realizadas por una filial con el acuerdo del proveedor. Los organismos notificados pondrán a disposición del público una lista de sus filiales.

4. Los documentos pertinentes relativos a la evaluación de las cualificaciones del subcontratista o de la filial y al trabajo realizado por éstos con arreglo al presente Reglamento se mantendrán a disposición de la autoridad notificante durante un período de 5 años a partir de la fecha de finalización de la actividad de subcontratación.

*Artículo 34 bis*

**Obligaciones operativas de los organismos notificados**

1. Los organismos notificados verificarán la conformidad del sistema de IA de alto riesgo con arreglo a los procedimientos de evaluación de la conformidad contemplados en el artículo 43.

2. Los organismos notificados desempeñarán sus actividades evitando cargas innecesarias a los proveedores y teniendo debidamente en cuenta el tamaño de la empresa, el sector en el que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate. Al hacerlo, el organismo notificado respetará, no obstante, el grado de rigor y el nivel de protección necesarios para que el sistema de IA de alto riesgo cumpla los requisitos del presente Reglamento. Se prestará especial atención a minimizar las cargas administrativas y los costes de cumplimiento para las microempresas y las pequeñas empresas, tal como se definen en la Recomendación 2003/361/CE de la Comisión.

3. Los organismos notificados pondrán a disposición de la autoridad notificante a que se refiere el artículo 30, y le presentarán cuando ésta lo solicite, toda la documentación pertinente, incluida la de los proveedores, para que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión y para facilitar la evaluación prevista en el presente capítulo.

*Artículo 35*

**Números de identificación y listas de organismos notificados designados en virtud del presente Reglamento**

1. La Comisión asignará un número de identificación a los organismos notificados. Asignará un único número, incluso cuando un organismo sea notificado en virtud de varios actos de la Unión.

2. La Comisión pondrá a disposición del público la lista de los organismos notificados en virtud del presente Reglamento, incluidos los números de identificación que les hayan sido asignados y las actividades para las que hayan sido notificados. La Comisión velará por que la lista se mantenga actualizada.

*Artículo 36*

**Cambios en las notificaciones**

-1. La autoridad notificante notificará a la Comisión y a los demás Estados miembros cualquier cambio pertinente en la notificación de un organismo notificado a través de la herramienta de notificación electrónica mencionada en el artículo 32, apartado 2.

-1 bis. Los procedimientos descritos en los artículos 31 y 32 se aplicarán a las ampliaciones del ámbito de aplicación de la notificación. Para las modificaciones de la notificación que no sean ampliaciones de su ámbito de aplicación, se aplicarán los procedimientos establecidos en los apartados siguientes.

Cuando un organismo notificado decida poner fin a sus actividades de evaluación de la conformidad, informará a la autoridad notificante y a los proveedores afectados lo antes posible y, en caso de cese previsto, un año antes del cese de sus actividades. Los certificados podrán seguir siendo válidos durante un período temporal de nueve meses tras el cese de las actividades del organismo notificado, a condición de que otro organismo notificado haya confirmado por escrito que asumirá la responsabilidad de los sistemas de IA cubiertos por dichos certificados. El nuevo organismo notificado completará una evaluación completa de los sistemas de IA afectados antes de que finalice dicho período, antes de expedir nuevos certificados para dichos sistemas. En caso de que el organismo notificado haya cesado su actividad, la autoridad notificante retirará la designación.

1. 1. Cuando una autoridad notificante tenga motivos suficientes para considerar que un organismo notificado ya no cumple los requisitos establecidos en el artículo 33 o que no está cumpliendo sus obligaciones, investigará el asunto sin demora y con la máxima diligencia. En este contexto, informará al organismo notificado en cuestión de las objeciones planteadas y le ofrecerá la posibilidad de dar a conocer su punto de vista. Si la autoridad notificante llega a la conclusión de que el organismo notificado ya no cumple los requisitos

establecido en el artículo 33 o que está incumpliendo sus obligaciones, restringirá, suspenderá o retirará la notificación, según proceda, en función de la gravedad del incumplimiento de dichos requisitos u obligaciones. Informará inmediatamente de ello a la Comisión y a los demás Estados miembros.

2 bis. En caso de suspensión, restricción o retirada total o parcial de su designación, el organismo notificado informará de ello a los fabricantes afectados en un plazo máximo de diez días.

2 ter. En caso de restricción, suspensión o retirada de una notificación, la autoridad notificante adoptará las medidas oportunas para que el organismo notificado conserve su expediente y lo ponga a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado cuando éstas lo soliciten.

2c. En caso de restricción, suspensión o retirada de una designación, la autoridad notificante deberá:

(a) evaluar el impacto en los certificados expedidos por el organismo notificado;

(b) presentar un informe sobre sus conclusiones a la Comisión y a los demás Estados miembros en un plazo de tres meses a partir de la notificación de las modificaciones;

(c) exigir al organismo notificado que suspenda o retire, en un plazo razonable determinado por la autoridad, los certificados que se hayan expedido indebidamente para garantizar la conformidad de los sistemas de IA en el mercado;

(d) informar a la Comisión y a los Estados miembros sobre los certificados cuya suspensión o retirada haya exigido;

(e) facilitará a las autoridades nacionales competentes del Estado miembro en el que el prestador tenga su domicilio social toda la información pertinente sobre los certificados cuya suspensión o retirada haya solicitado. Dicha autoridad competente tomará las medidas adecuadas, en caso necesario, para evitar un riesgo potencial para la salud, la seguridad o los derechos fundamentales.

2d. Con excepción de los certificados expedidos indebidamente, y cuando una notificación haya sido suspendida o restringida, los certificados seguirán siendo válidos en las siguientes circunstancias:

(a) la autoridad notificante ha confirmado, en el plazo de un mes a partir de la suspensión o restricción, que no existe riesgo para la salud, la seguridad o los derechos fundamentales en relación con los certificados afectados por la suspensión o restricción, y la autoridad notificante ha esbozado un calendario y las medidas previstas para poner remedio a la suspensión o restricción; o bien

la autoridad notificante ha confirmado que no se expedirán, modificarán o reexpedirán certificados pertinentes para la suspensión durante el transcurso de la suspensión o restricción, y declara si el organismo notificado tiene capacidad para seguir supervisando y seguir siendo responsable de los certificados existentes expedidos durante el período de la suspensión o restricción. En caso de que la autoridad responsable de los organismos notificados determine que el organismo notificado no tiene capacidad para respaldar los certificados existentes expedidos, el proveedor facilitará a las autoridades nacionales competentes del Estado miembro en el que tenga su domicilio social el proveedor del sistema objeto del certificado, en un plazo de tres meses a partir de la suspensión o restricción, una confirmación por escrito de que otro organismo notificado cualificado está asumiendo temporalmente las funciones del organismo notificado para supervisar y seguir siendo responsable de los certificados durante el período de suspensión o restricción.

2e. Con excepción de los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados seguirán siendo válidos durante un periodo de nueve meses en las siguientes circunstancias:

(a) cuando la autoridad nacional competente del Estado miembro en el que tenga su domicilio social el proveedor del sistema de IA objeto del certificado haya confirmado que no existen riesgos para la salud, la seguridad y los derechos fundamentales asociados a los sistemas en cuestión; y

(b) otro organismo notificado haya confirmado por escrito que asumirá inmediatamente la responsabilidad de dichos sistemas y que habrá finalizado la evaluación de los mismos en un plazo de doce meses a partir de la retirada de la designación.

En las circunstancias contempladas en el párrafo primero, la autoridad nacional competente del Estado miembro en el que tenga su sede el proveedor del sistema objeto del certificado podrá prorrogar la validez provisional de los certificados por períodos adicionales de tres meses, que en total no superarán los doce meses.

2 septies. La autoridad nacional competente o el organismo notificado que asuma las funciones del organismo notificado afectado por el cambio de notificación informará inmediatamente de ello a la Comisión, a los demás Estados miembros y a los demás organismos notificados.

*Artículo 37*

**Impugnación de la competencia de los organismos notificados**

1. La Comisión investigará, en caso necesario, todos los casos en que existan razones para dudar de la competencia de un organismo notificado o del cumplimiento continuado por parte de un organismo notificado de los requisitos establecidos en el artículo 33 y de sus responsabilidades aplicables.

2. La autoridad notificante facilitará a la Comisión, a petición de ésta, toda la información pertinente sobre la notificación o el mantenimiento de la competencia del organismo notificado en cuestión.

3. La Comisión velará por que toda la información sensible obtenida en el curso de sus investigaciones con arreglo al presente artículo sea tratada confidencialmente de conformidad con el artículo 70.

4. Cuando la Comisión compruebe que un organismo notificado no cumple o ha dejado de cumplir los requisitos de su notificación, informará al Estado miembro notificante al respecto y le pedirá que adopte las medidas correctoras necesarias, que pueden consistir, si es necesario, en la suspensión o retirada de la notificación. Si el Estado miembro no adopta las medidas correctoras necesarias, la Comisión podrá, mediante actos de ejecución, suspender, restringir o retirar la designación. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 74, apartado 2.

*Artículo 38*

**Coordinación de los organismos notificados**

1. La Comisión velará por que, en lo que respecta a los sistemas de IA de alto riesgo, se establezca y funcione adecuadamente una coordinación y cooperación adecuadas entre los organismos notificados activos en los procedimientos de evaluación de la conformidad con arreglo al presente Reglamento en forma de grupo sectorial de organismos notificados.

2. La autoridad notificante se asegurará de que los organismos que haya notificado participan en los trabajos del grupo, directamente o por medio de representantes designados.

2 bis. La Comisión preverá el intercambio de conocimientos y mejores prácticas entre las autoridades de notificación de los Estados miembros.

*Artículo 39*

**Organismos de evaluación de la conformidad de terceros países**

Los organismos de evaluación de la conformidad establecidos con arreglo a la legislación de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados a realizar las actividades de los organismos notificados en virtud del presente Reglamento, siempre que cumplan los requisitos del artículo 33 o garanticen un nivel de cumplimiento equivalente.

# Capítulo 5
# NORMAS, EVALUACIÓN DE LA CONFORMIDAD, CERTIFICADOS, REGISTRO

*Artículo 40*

**Normas armonizadas y resultados de la normalización**

1. Se presumirá que los sistemas de IA de alto riesgo o los modelos de IA de propósito general que sean conformes con las normas armonizadas o partes de las mismas cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea de conformidad con el Reglamento (UE) 1025/2012 son conformes con los requisitos establecidos en el capítulo 2 del presente título o, según proceda, con los requisitos establecidos en el [capítulo sobre el IPAM], en la medida en que dichas normas cubran esos requisitos.

2. La Comisión emitirá sin demora indebida solicitudes de normalización que cubran todos los requisitos del título II, capítulo III y, en su caso, [capítulo GPAI] del presente Reglamento, de conformidad con el artículo 10 del Reglamento (UE) nº 1025/2012. En la solicitud de normalización también se pedirán resultados sobre los procesos de información y documentación para mejorar el rendimiento de los recursos de los sistemas de IA, como la reducción del consumo de energía y otros recursos del sistema de IA de alto riesgo durante su ciclo de vida, y sobre el desarrollo energéticamente eficiente de modelos de IA de propósito general. Al preparar la solicitud de normalización, la Comisión consultará al Consejo y a las partes interesadas pertinentes, incluido el Foro Consultivo.

Al formular una solicitud de normalización a las organizaciones europeas de normalización, la Comisión especificará que las normas han de ser coherentes, incluso con las normas existentes y futuras desarrolladas en los distintos sectores para los productos cubiertos por la legislación vigente de la Unión en materia de seguridad enumerada en el anexo II, claras y destinadas a garantizar que los sistemas de IA o

los modelos comercializados o puestos en servicio en la Unión cumplen los requisitos pertinentes establecidos en el presente Reglamento.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de sus mejores esfuerzos para cumplir los objetivos mencionados, de conformidad con el artículo 24 del Reglamento UE 1025/2012.

1 quaterLos agentes implicados en el proceso de normalización tratarán de promover la inversión y la innovación en la IA, incluso mediante el aumento de la seguridad jurídica, así como la competitividad y el crecimiento del mercado de la Unión, y contribuirán a reforzar la cooperación mundial en materia de normalización y teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que sean coherentes con los valores, los derechos fundamentales y los intereses de la Unión, y mejorarán la gobernanza multilateral garantizando una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) n.º 1025/2012.

*Artículo 41*

**Especificaciones comunes**

1. La Comisión estará facultada para adoptar, previa consulta al Foro Consultivo a que se refiere el artículo 58 bis, actos de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2, por los que se establezcan especificaciones comunes para los requisitos establecidos en el capítulo 2 del presente título o, según proceda, con los requisitos establecidos en el artículo [capítulo GPAI], para los sistemas de IA incluidos en el ámbito de aplicación del presente Reglamento, cuando se cumplan las siguientes condiciones:

(a) la Comisión haya solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en el capítulo 2 del presente título; y

(i) la solicitud no ha sido aceptada por ninguno de los organismos europeos de normalización; o

(ii) las normas armonizadas que atiendan a dicha solicitud no se entreguen en el plazo establecido de conformidad con el artículo 10, apartado 1, del Reglamento 1025/2012; o bien

(iii) las normas armonizadas pertinentes no abordan suficientemente los problemas relacionados con los derechos fundamentales; o

(iv) las normas armonizadas no se ajustan a lo solicitado; y

no se ha publicado en el Diario Oficial de la Unión Europea ninguna referencia a normas armonizadas que cubran los requisitos contemplados en el capítulo II del presente título, de conformidad con el Reglamento (UE) no 1025/2012, y no se espera que se publique tal referencia en un plazo razonable.

1 bis. Antes de preparar un proyecto de acto de ejecución, la Comisión informará al comité mencionado en el artículo 22 del Reglamento UE (n.º) 1025/2012 de que considera que se cumplen las condiciones del apartado 1.

3. 2. Se presumirá que los sistemas de IA de alto riesgo que sean conformes con las especificaciones comunes a que se refiere el apartado 1, o con partes de las mismas, son conformes con los requisitos establecidos en el capítulo 2 del presente título, en la medida en que dichas especificaciones comunes cubran dichos requisitos.

3 bis. Cuando un organismo europeo de normalización adopte una norma armonizada y proponga a la Comisión la publicación de su referencia en el Diario Oficial de la Unión Europea, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) no 1025/2012. Cuando se publique la referencia de una norma armonizada en el Diario Oficial de la Unión Europea, la Comisión derogará los actos a que se refieren los apartados 1 y 1 ter, o partes de los mismos, que cubran los mismos requisitos establecidos en el capítulo 2 del presente título.

4. Cuando los proveedores de sistemas de IA de alto riesgo no cumplan las especificaciones comunes a que se refiere el apartado 1, deberán justificar debidamente que han adoptado soluciones técnicas que cumplen los requisitos contemplados en el capítulo II a un nivel al menos equivalente a los mismos.

4 ter. Cuando un Estado miembro considere que un pliego de condiciones común no satisface plenamente los requisitos establecidos en el capítulo 2 del presente título, informará de ello a la Comisión con una explicación detallada y la Comisión evaluará dicha información y, si procede, modificará el acto de ejecución por el que se establece el pliego de condiciones común en cuestión.

*Artículo 42*

**Presunción de conformidad con determinados requisitos**

1. Sistemas de IA de alto riesgo que han sido entrenados y probados con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico al que están destinados.

se presumirá que cumplen los requisitos respectivos establecidos en el apartado 4 del artículo 10.

2. Se presumirá que los sistemas de IA de alto riesgo que hayan sido certificados o para los que se haya emitido una declaración de conformidad en virtud de un régimen de ciberseguridad con arreglo al Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[1] y cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea cumplen los requisitos de ciberseguridad establecidos en el artículo 15 del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad o partes de los mismos cubran dichos requisitos.

*Artículo 43*

**Evaluación de la conformidad**

1. En el caso de los sistemas de IA de alto riesgo enumerados en el punto 1 del anexo III, cuando, al demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, el proveedor haya aplicado las normas armonizadas a que se refiere el artículo 40 o, en su caso, las especificaciones comunes a que se refiere el artículo 41, el proveedor optará por uno de los siguientes procedimientos:

(a) el procedimiento de evaluación de la conformidad basado en el control interno contemplado en el Anexo VI; o

(b) el procedimiento de evaluación de la conformidad basado en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica, con la participación de un organismo notificado, contemplado en el anexo VII.

Para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, el proveedor seguirá el procedimiento de evaluación de la conformidad establecido en el anexo VII en los siguientes casos:

(a) cuando no existan las normas armonizadas a que se refiere el artículo 40 y no se disponga de las especificaciones comunes a que se refiere el artículo 41;

(aa) el prestador no ha aplicado o sólo ha aplicado parcialmente la norma armonizada;

(b) cuando existan las especificaciones comunes mencionadas en la letra a) pero el proveedor no las haya aplicado;

(c) cuando una o varias de las normas armonizadas mencionadas en la letra a) se hayan publicado con una restricción y sólo en la parte de la norma que se haya restringido.

A efectos del procedimiento de evaluación de la conformidad contemplado en el Anexo VII, el proveedor podrá elegir cualquiera de los organismos notificados. No obstante, cuando el sistema esté destinado a ser puesto en servicio por autoridades policiales, de inmigración o asilo, así como por instituciones, órganos u organismos de la UE, actuará como organismo notificado la autoridad de vigilancia del mercado a que se refiere el artículo 63, apartados 5 o 6, según proceda.

2. Para los sistemas de IA de alto riesgo contemplados en los puntos 2 a 8 del Anexo III, los proveedores seguirán el procedimiento de evaluación de la conformidad basado en el control interno contemplado en el Anexo VI, que no prevé la participación de un organismo notificado.

3. En el caso de los sistemas de IA de alto riesgo a los que se apliquen los actos jurídicos enumerados en la sección A del anexo II, el proveedor llevará a cabo la evaluación de la conformidad pertinente con arreglo a lo dispuesto en dichos actos jurídicos. Los requisitos establecidos en el capítulo 2 del presente título se aplicarán a dichos sistemas de IA de alto riesgo y formarán parte de dicha evaluación. Los puntos 4.3., 4.4., 4.5. y el quinto párrafo del punto

4.6 del Anexo VII.

A efectos de dicha evaluación, los organismos notificados que hayan sido notificados con arreglo a dichos actos jurídicos tendrán derecho a controlar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, siempre que el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 33, apartados 4, 9 y 10, haya sido evaluado en el contexto del procedimiento de notificación con arreglo a dichos actos jurídicos.

Cuando los actos jurídicos enumerados en el anexo II, sección A, permitan al fabricante del producto renunciar a una evaluación de la conformidad por terceros, siempre que dicho fabricante haya aplicado todas las normas armonizadas que cubran todos los requisitos pertinentes, dicho fabricante sólo podrá hacer uso de esa opción si también ha aplicado las normas armonizadas o, en su caso, las especificaciones comunes a que se refiere el artículo 41, que cubran los requisitos establecidos en el capítulo 2 del presente título.

4. Los sistemas de IA de alto riesgo que ya hayan sido sometidos a un procedimiento de evaluación de la conformidad deberán someterse a un nuevo procedimiento de evaluación de la conformidad cada vez que se modifiquen sustancialmente, independientemente de si el sistema modificado está destinado a ser distribuido ulteriormente o sigue siendo utilizado por el implantador actual.

En el caso de los sistemas de IA de alto riesgo que sigan aprendiendo después de su comercialización o puesta en servicio, los cambios en el sistema de IA de alto riesgo y en sus prestaciones que hayan sido determinados previamente por el proveedor en el momento de la evaluación inicial de la conformidad y formen parte de la información contenida en la documentación técnica a que se refiere el anexo IV, punto 2, letra f), no constituirán una modificación sustancial.

Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73 a fin de actualizar los anexos VI y VII a la luz del progreso técnico.

5. Se otorgan a la Comisión los poderes para adoptar actos delegados a fin de modificar los apartados 1 y 2 con objeto de someter los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 2 a 8, al procedimiento de evaluación de la conformidad a que se refiere el anexo VII o a partes del mismo. La Comisión adoptará dichos actos delegados teniendo en cuenta la eficacia del procedimiento de evaluación de la conformidad basado en el control interno a que se refiere el anexo VI para prevenir o reducir al mínimo los riesgos para la salud y la seguridad y la protección de los derechos fundamentales que plantean dichos sistemas, así como la disponibilidad de capacidades y recursos adecuados entre los organismos notificados.

*Artículo 44*

**Certificados**

1. Los certificados expedidos por los organismos notificados de conformidad con el Anexo VII se redactarán en una lengua fácilmente comprensible para las autoridades competentes del Estado miembro en el que esté establecido el organismo notificado.

2. Los certificados serán válidos durante el período que indiquen, que no excederá de cinco años para los sistemas de IA contemplados en el Anexo II y de cuatro años para los sistemas de IA contemplados en el Anexo III. Previa solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales, cada uno de los cuales no excederá de cinco años para los sistemas de IA cubiertos por el Anexo II y de cuatro años para los sistemas de IA cubiertos por el Anexo III, sobre la base de una reevaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables. Todo suplemento de un certificado seguirá siendo válido mientras lo sea el certificado al que suplementa.

3. Si un organismo notificado comprueba que un sistema de IA ya no cumple los requisitos establecidos en el capítulo 2 del presente título, suspenderá o retirará el certificado expedido o le impondrá restricciones, teniendo en cuenta el principio de proporcionalidad, a menos que el proveedor del sistema garantice el cumplimiento de dichos requisitos mediante la adopción de medidas correctoras adecuadas en un plazo adecuado fijado por el organismo notificado. El organismo notificado motivará su decisión.

Deberá existir un procedimiento de recurso contra las decisiones de los organismos notificados, incluidos los certificados de conformidad expedidos.

*Artículo 46*

**Obligaciones de información de los organismos notificados**

1. Los organismos notificados informarán a la autoridad notificante de lo siguiente

(a) los certificados de evaluación de la documentación técnica de la Unión, los suplementos de dichos certificados y las aprobaciones de sistemas de gestión de la calidad expedidos de conformidad con los requisitos del Anexo VII;

(b) cualquier denegación, restricción, suspensión o retirada de un certificado de evaluación de la documentación técnica de la Unión o de una aprobación de un sistema de gestión de la calidad expedidos de conformidad con los requisitos del anexo VII;

(c) cualquier circunstancia que afecte al alcance o a las condiciones de la notificación;

(d) cualquier solicitud de información que hayan recibido de las autoridades de vigilancia del mercado en relación con las actividades de evaluación de la conformidad;

(e) previa solicitud, las actividades de evaluación de la conformidad realizadas en el ámbito de su notificación y cualquier otra actividad realizada, incluidas las actividades transfronterizas y la subcontratación.

2. Cada organismo notificado informará a los demás organismos notificados de:

(a) las aprobaciones de sistemas de gestión de la calidad que haya denegado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de calidad que haya expedido;

(b) Certificados de evaluación de la documentación técnica de la UE o cualquier suplemento de los mismos que haya denegado, retirado, suspendido o restringido de otro modo, y, previa solicitud, de los certificados y/o suplementos de los mismos que haya expedido.

3. Cada organismo notificado proporcionará a los demás organismos notificados que realicen actividades similares de evaluación de la conformidad que abarquen los mismos tipos de sistemas de IA información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de la evaluación de la conformidad.

3a. Las obligaciones contempladas en los apartados 1 a 3 se cumplirán de conformidad con el artículo 70.

*Artículo 47*

**Excepción al procedimiento de evaluación de la conformidad**

1. No obstante lo dispuesto en el artículo 43 y previa solicitud debidamente justificada, cualquier autoridad de vigilancia del mercado podrá autorizar la introducción en el mercado o la puesta en servicio de sistemas específicos de IA de alto riesgo en el territorio del Estado miembro de que se trate, por motivos excepcionales de seguridad pública o de protección de la vida y la salud de las personas, protección del medio ambiente y protección de activos industriales e infraestructurales clave. Dicha autorización tendrá una duración limitada mientras se llevan a cabo los procedimientos necesarios de evaluación de la conformidad, teniendo en cuenta las razones excepcionales que justifican la excepción. La conclusión de dichos procedimientos se llevará a cabo sin demoras indebidas.

1 bis. En una situación de urgencia debidamente justificada por razones excepcionales de seguridad pública o en caso de amenaza específica, sustancial e inminente para la vida o la seguridad física de las personas físicas, las fuerzas y cuerpos de seguridad o las autoridades de protección civil podrán poner en servicio un sistema específico de IA de alto riesgo sin la autorización a que se refiere el apartado 1, siempre que dicha autorización se solicite durante o después de la utilización sin demora indebida, y si se deniega dicha autorización, se interrumpirá su utilización con efecto inmediato y se desecharán inmediatamente todos los resultados y productos de dicha utilización.

2. 2. La autorización a que se refiere el apartado 1 sólo se expedirá si la autoridad de vigilancia del mercado llega a la conclusión de que el sistema de IA de alto riesgo cumple los requisitos del capítulo 2 del presente título. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida con arreglo al apartado 1. Esta obligación no cubrirá los datos operativos sensibles en relación con las actividades de las autoridades policiales.

3. Cuando, en el plazo de 15 días naturales a partir de la recepción de la información a que se refiere el apartado 2, ni un Estado miembro ni la Comisión hayan planteado objeciones a una autorización expedida por una autoridad de vigilancia del mercado de un Estado miembro de conformidad con el apartado 1, dicha autorización se considerará justificada.

4. Cuando, en el plazo de 15 días naturales a partir de la recepción de la notificación a que se refiere el apartado 2, un Estado miembro formule objeciones contra una autorización expedida por una autoridad de vigilancia del mercado de otro Estado miembro, o cuando la Comisión considere que la autorización es contraria al Derecho de la Unión o que la conclusión de los Estados miembros sobre la conformidad del sistema a que se refiere el apartado 2 es infundada, la

La Comisión consultará sin demora al Estado miembro de que se trate; el operador u operadores afectados serán consultados y tendrán la posibilidad de presentar sus puntos de vista. En vista de ello, la Comisión decidirá si la autorización está justificada o no. La Comisión dirigirá su decisión al Estado miembro interesado y al operador u operadores correspondientes.

5. Si la autorización se considera injustificada, la autoridad de vigilancia del mercado del Estado miembro en cuestión la retirará.

6. Para los sistemas de IA de alto riesgo relacionados con productos cubiertos por la legislación de armonización de la Unión mencionada en el anexo II, sección A, sólo se aplicarán los procedimientos de excepción de evaluación de la conformidad establecidos en dicha legislación.

*Artículo 48*

**Declaración de conformidad de la UE**

1. El proveedor redactará una declaración UE de conformidad, legible por máquina, física o firmada electrónicamente, para cada sistema de IA de alto riesgo y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años a partir de la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo. En la declaración UE de conformidad se identificará el sistema de IA de alto riesgo para el que ha sido elaborada. Previa solicitud, se presentará una copia de la declaración UE de conformidad a las autoridades nacionales competentes pertinentes.

2. La declaración UE de conformidad afirmará que el sistema de IA de alto riesgo en cuestión cumple los requisitos establecidos en el capítulo 2 del presente título. 2. La declaración UE de conformidad contendrá la información establecida en el anexo V y se traducirá a una lengua fácilmente comprensible para las autoridades nacionales competentes de los Estados miembros en los que se comercialice o se ponga a disposición el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sujetos a otra legislación de armonización de la Unión que también requiera una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a toda la legislación de la Unión aplicable al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para la identificación de la legislación de armonización de la Unión a la que se refiere la declaración.

4. Al elaborar la declaración UE de conformidad, el proveedor asumirá la responsabilidad del cumplimiento de los requisitos establecidos en el capítulo 2 del presente título. El proveedor mantendrá actualizada la declaración UE de conformidad según proceda.

La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 73 a fin de actualizar el contenido de la declaración UE de conformidad establecida en el anexo V para introducir elementos que resulten necesarios a la luz del progreso técnico.

*Artículo 49*

**Marcado CE de conformidad**

1. El marcado CE de conformidad estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) nº 765/2008.

1 bis. En el caso de los sistemas de IA de alto riesgo suministrados digitalmente, se utilizará un marcado CE digital sólo si se puede acceder fácilmente a él a través de la interfaz desde la que se accede al sistema de IA o a través de un código legible por máquina de fácil acceso u otro medio electrónico.

2. El marcado CE se colocará de manera visible, legible e indeleble en los sistemas de IA de alto riesgo. Cuando ello no sea posible o no pueda garantizarse debido a la naturaleza del sistema de IA de alto riesgo, se colocará en el embalaje o en la documentación adjunta, según proceda.

3. Cuando proceda, el marcado CE irá seguido del número de identificación del organismo notificado responsable de los procedimientos de evaluación de la conformidad establecidos en el artículo 43. El número de identificación del organismo notificado será colocado por el propio organismo o, siguiendo sus instrucciones, por el proveedor o su representante autorizado. El número de identificación se indicará asimismo en todo material de promoción en el que se mencione que el sistema de IA de alto riesgo cumple los requisitos para el marcado CE.

3 bis. Cuando los sistemas de IA de alto riesgo estén sujetos a otra legislación de la Unión que también prevea la colocación del marcado CE, éste indicará que el sistema de IA de alto riesgo también cumple los requisitos de esa otra legislación.

*Artículo 51*

**Inscripción**

1. Antes de comercializar o poner en servicio un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo a que se refiere el punto 2 del anexo III, el proveedor o, en su caso, el representante autorizado se registrará a sí mismo y a su sistema en la base de datos de la UE a que se refiere el artículo 60.

1a. Antes de comercializar o poner en servicio un sistema de IA para el que el proveedor haya llegado a la conclusión de que no es de alto riesgo en aplicación del procedimiento previsto en el apartado 2 bis del artículo 6, el proveedor o, en su caso, el representante autorizado se registrará a sí mismo y a dicho sistema en la base de datos de la UE a que se refiere el artículo 60.

1 ter. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo enumerados en el punto 2 del anexo III, los responsables del despliegue que sean autoridades, agencias u organismos públicos o personas que actúen en su nombre se registrarán, seleccionarán el sistema y registrarán su uso en la base de datos de la UE a que se refiere el artículo 60.

1 quater. Para los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del Anexo III en los ámbitos de la aplicación de la ley, la migración, el asilo y la gestión del control fronterizo, el registro a que se refieren los apartados 1 a 1 ter se efectuará en una sección segura no pública de la base de datos de la UE a que se refiere el artículo 60 e incluirá únicamente la siguiente información, según proceda:

- los puntos 1 a 9 de la sección A del anexo VIII, con excepción de los puntos 5a, 7 y 8;
- puntos 1 a 3 de la sección B del anexo VIII;
- los puntos 1 a 9 de la sección X del anexo VIII, con excepción de los puntos 6 y 7;
- los puntos 1 a 5 del anexo VIII bis, con excepción del punto 4.

Sólo la Comisión y las autoridades nacionales mencionadas en el art. 63(5) tendrán acceso a estas secciones restringidas de la base de datos de la UE.

1d.Los sistemas de IA de alto riesgo a que se refiere el punto 2 del Anexo III se registrarán a escala nacional.

# TÍTULO IV

# OBLIGACIONES DE TRANSPARENCIA PARA LOS PROVEEDORES E IMPLANTADORES DE DETERMINADOS SISTEMAS DE AI

*Artículo 52*

**Obligaciones de transparencia para proveedores y usuarios de determinados sistemas de IA y modelos GPAI**

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de forma que las personas físicas afectadas sean informadas de que están interactuando con un sistema de IA, a menos que ello resulte obvio desde el punto de vista de una persona física razonablemente bien informada, observadora y perspicaz, teniendo en cuenta las circunstancias y el contexto de uso. Esta obligación no se aplicará a la IA

los sistemas autorizados por la ley para detectar, prevenir, investigar y enjuiciar delitos, sin perjuicio de las salvaguardias adecuadas de los derechos y libertades de terceros, a menos que dichos sistemas estén a disposición del público para denunciar un delito.

1 bis. Los proveedores de sistemas de IA, incluidos los sistemas GPAI, que generen contenidos sintéticos de audio, imagen, vídeo o texto, garantizarán que los resultados del sistema de IA estén marcados en un formato legible por máquina y detectable como generado o manipulado artificialmente. Los proveedores garantizarán que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las especificidades y limitaciones de los diferentes tipos de contenidos, los costes de aplicación y el estado de la técnica generalmente reconocido, tal como pueda reflejarse en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA realicen una función de asistencia para la edición estándar o no alteren sustancialmente los datos de entrada proporcionados por el usuario o la semántica de los mismos, o cuando estén autorizados por ley para detectar, prevenir, investigar y perseguir delitos penales.

2. Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas al mismo y tratarán los datos personales de conformidad con el Reglamento (UE) 2016/679, el Reglamento (UE) 2016/1725 y la Directiva (UE) 2016/280, según proceda. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones, permitidos por la ley para detectar, prevenir e investigar delitos penales, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, y de conformidad con el Derecho de la Unión.

3. Los implantadores de un sistema de IA que genere o manipule contenidos de imagen, audio o vídeo que constituyan una falsificación profunda, deberán revelar que el contenido ha sido generado o manipulado artificialmente. Esta obligación no se aplicará cuando el uso esté autorizado por la ley para detectar, prevenir, investigar y perseguir delitos penales. Cuando el contenido forme parte de una obra o programa evidentemente artístico, creativo, satírico o análogo de ficción, las obligaciones de transparencia establecidas en el presente apartado se limitarán a revelar la existencia de dicho contenido generado o manipulado de una manera adecuada que no obstaculice la visualización o el disfrute de la obra.

Los usuarios de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público deberán revelar que el texto ha sido generado o manipulado artificialmente. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar y enjuiciar delitos o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o control editorial y

cuando una persona física o jurídica tenga la responsabilidad editorial de la publicación del contenido.

3a. La información a que se refieren los apartados 1 a 3 se facilitará a las personas físicas afectadas de forma clara y distinguible a más tardar en el momento de la primera interacción o exposición. La información respetará los requisitos de accesibilidad aplicables.

4. Los apartados 1, 2 y 3 no afectarán a los requisitos y obligaciones establecidos en el título III del presente Reglamento y se entenderán sin perjuicio de otras obligaciones de transparencia para los usuarios de sistemas de IA establecidas en la legislación de la Unión o nacional.

4 bis.La Oficina de AI fomentará y facilitará la elaboración de códigos de prácticas a escala de la Unión para facilitar la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados artificialmente. La Comisión estará facultada para adoptar actos de ejecución para aprobar estos códigos de prácticas de conformidad con el procedimiento establecido en los apartados 6 a 8 del artículo 52 sexies. Si considera que el código no es adecuado, la Comisión estará facultada para adoptar un acto de ejecución que especifique las normas comunes para la aplicación de dichas obligaciones de conformidad con el procedimiento de examen establecido en el artículo 73, apartado 2.

# TÍTULO VIIIA MODELOS AI DE PROPÓSITO GENERAL

## Capítulo 1 NORMAS DE CLASIFICACIÓN

*Artículo 52 bis*

**Clasificación de los modelos de IA de propósito general como modelos de IA de propósito general con riesgo sistémico**

1. Un modelo de IA de propósito general se clasificará como modelo de IA de propósito general con riesgo sistémico si cumple alguno de los siguientes criterios:

(a) tiene capacidades de alto impacto evaluadas sobre la base de herramientas técnicas y metodologías apropiadas, incluidos indicadores y puntos de referencia;

basándose en una decisión de la Comisión, de oficio o tras una alerta cualificada de la comisión técnica científica, de que un modelo de IA de propósito general tiene capacidades o repercusiones equivalentes a las de la letra a).

2. Se presumirá que un modelo de IA de propósito general tiene capacidades de alto impacto con arreglo a la letra a) del apartado 1 cuando la cantidad acumulada de cálculo utilizada para su entrenamiento medida en operaciones en coma flotante (FLOPs) sea superior a 10^25.

3. La Comisión adoptará actos delegados de conformidad con el artículo 73, apartado 2, para modificar los umbrales enumerados en los apartados anteriores, así como para complementar los puntos de referencia e indicadores a la luz de la evolución tecnológica, como las mejoras algorítmicas o el aumento de la eficiencia del hardware, cuando sea necesario, para que estos umbrales reflejen el estado de la técnica.

*Artículo 52 ter*

**Procedimiento**

1. Cuando un modelo de IA de propósito general cumpla los requisitos contemplados en el artículo 52 bis, apartado 1, letra a), el proveedor pertinente lo notificará a la Comisión sin demora y, en cualquier caso, en el plazo de dos semanas a partir del momento en que se cumplan dichos requisitos o se tenga conocimiento de que se cumplirán. Dicha notificación incluirá la información necesaria para demostrar que se han cumplido los requisitos pertinentes. Si la Comisión tiene conocimiento de que un modelo de IA de propósito general presenta riesgos sistémicos de los que no ha sido notificada, podrá decidir designarlo como modelo con riesgo sistémico.

2. El proveedor de un modelo de IA de propósito general que cumpla los requisitos contemplados en el artículo 52 bis, apartado 1, letra a), podrá presentar, junto con su notificación, argumentos suficientemente fundamentados para demostrar que, excepcionalmente, aunque cumpla dichos requisitos, el modelo de IA de propósito general no presenta, por sus características específicas, riesgos sistémicos y, por tanto, no debe clasificarse como modelo de IA de propósito general con riesgo sistémico.

3. Cuando la Comisión llegue a la conclusión de que los argumentos presentados con arreglo al apartado 2 no están suficientemente fundamentados y el proveedor pertinente no haya podido demostrar que el modelo de IA de propósito general no presenta, debido a sus características específicas, riesgos sistémicos, rechazará dichos argumentos y el modelo de IA de propósito general se considerará modelo de IA de propósito general con riesgo sistémico.

La Comisión podrá designar un modelo de IA de propósito general como modelo que presenta riesgos sistémicos, de oficio o a raíz de una alerta cualificada de la comisión técnica científica de conformidad con el artículo 68 nonies, letra a) [*Alertas de riesgos sistémicos por la comisión técnica científica*] (1) , sobre la base de los criterios establecidos en el anexo IX quater. La Comisión estará facultada para especificar y actualizar los criterios del anexo IX quater mediante actos delegados, de conformidad con el artículo 74, apartado 2.

4 bis. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de propósito general con riesgo sistémico con arreglo al apartado 4, la Comisión tendrá en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de propósito general presenta riesgos sistémicos sobre la base de los criterios establecidos en el anexo IX quater. Dicha solicitud deberá contener razones objetivas, concretas y nuevas que hayan surgido desde la decisión de designación. Los proveedores podrán solicitar la reevaluación como muy pronto seis meses después de la decisión de designación. Cuando la Comisión, tras su reevaluación, decida mantener la designación como modelo de IA de propósito general con riesgo sistémico, los proveedores podrán solicitar una reevaluación como muy pronto seis meses después de esta decisión.

4. La Comisión velará por que se publique una lista de modelos de IA de propósito general con riesgo sistémico y mantendrá actualizada dicha lista, sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

# Capítulo 2

# OBLIGACIONES PARA LOS PROVEEDORES DE MODELOS AI DE USO GENERAL

*Artículo 52 quater*

**Obligaciones de los proveedores de modelos de IA de propósito general**

1. Los proveedores de modelos de IA de propósito general deberán:

(a) elaborará y mantendrá actualizada la documentación técnica del modelo, incluido su proceso de formación y ensayo y los resultados de su evaluación, que contendrá, como mínimo, los elementos establecidos en el anexo IX bis con el fin de facilitarla, previa solicitud, a la Oficina de AI y a las autoridades nacionales competentes;

(b) elaborar, mantener al día y facilitar información y documentación a los proveedores de sistemas de IA que pretendan integrar el modelo de IA de propósito general en

su sistema de IA. Sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional, la información y la documentación deberán:

(i) permitir a los proveedores de sistemas de IA conocer bien las capacidades y limitaciones del modelo de IA de propósito general y cumplir las obligaciones que les impone el presente Reglamento; y

(ii) contener, como mínimo, los elementos que figuran en el anexo IX ter.

(c) establecer una política de respeto de la legislación de la Unión en materia de derechos de autor, en particular para identificar y respetar, incluso mediante las tecnologías más avanzadas, las reservas de derechos expresadas de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790;

(d) elaborar y poner a disposición del público un resumen suficientemente detallado sobre el contenido utilizado para el entrenamiento del modelo de IA de propósito general, de acuerdo con una plantilla facilitada por la Oficina de IA.

-2. Las obligaciones establecidas en el apartado 1, con excepción de las letras c) y d), no se aplicarán a los proveedores de modelos de IA que se pongan a disposición del público bajo una licencia libre y abierta que permita el acceso, uso, modificación y distribución del modelo, y cuyos parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Esta excepción no se aplicará a los modelos de IA de propósito general con riesgos sistémicos.

2. Los proveedores de modelos de IA de propósito general cooperarán en la medida necesaria con la Comisión y las autoridades nacionales competentes en el ejercicio de sus competencias y facultades con arreglo al presente Reglamento.

3. Los proveedores de modelos de IA de propósito general podrán basarse en códigos de buenas prácticas en el sentido del artículo 52 sexies para demostrar el cumplimiento de las obligaciones del apartado 1, hasta que se publique una norma armonizada. El cumplimiento de una norma armonizada europea otorga a los proveedores la presunción de conformidad. Los proveedores de modelos de IA de propósito general con riesgos sistémicos que no se adhieran a un código de buenas prácticas aprobado deberán demostrar medios alternativos adecuados de cumplimiento para su aprobación por la Comisión.

4. A fin de facilitar el cumplimiento del anexo IX bis, en particular el punto 2, letras d) y e), la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 73 para detallar las metodologías de medición y cálculo con vistas a permitir una documentación comparable y verificable.

4 bis.Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73, apartado 2, para modificar los anexos IX bis y IX ter a la luz de la evolución tecnológica.

4b. Toda información y documentación obtenida en virtud de lo dispuesto en el presente artículo, incluidos los secretos comerciales, se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 70.

*Artículo 52 quater bis*

**Representante autorizado**

1. Antes de introducir un modelo de IA de propósito general en el mercado de la Unión, los proveedores establecidos fuera de la Unión designarán, mediante mandato escrito, a un representante autorizado que esté establecido en la Unión y que le permita desempeñar las funciones que le atribuye el presente Reglamento.

2. El representante autorizado realizará las tareas especificadas en el mandato recibido del proveedor. Facilitará una copia del mandato a la Oficina de AI, a petición de ésta, en una de las lenguas oficiales de las instituciones de la Unión. A efectos del presente Reglamento, el mandato facultará al representante autorizado para llevar a cabo las siguientes tareas:

(a) comprobar que se ha elaborado la documentación técnica especificada en el anexo IX bis y que se han cumplido todas las obligaciones a que se refieren los artículos 52 quater y, en su caso, el artículo

52dhan sido cumplidas por el proveedor;

(b) conservar una copia de la documentación técnica a disposición de la Oficina AI y de las autoridades nacionales competentes, durante un período que finalizará diez años después de la comercialización del modelo, así como los datos de contacto del proveedor que haya designado al representante autorizado;

(c) facilitar a la Oficina de AI, previa solicitud motivada, toda la información y documentación, incluida la conservada con arreglo a la letra a), necesaria para demostrar el cumplimiento de las obligaciones del presente Título;

(d) cooperar con la Oficina de Inteligencia Artificial y las autoridades nacionales competentes, previa solicitud motivada, en cualquier acción que estas últimas emprendan en relación con el modelo de IA de propósito general con riesgos sistémicos, incluso cuando el modelo se integre en sistemas de IA

comercializados o puestos en servicio en la Unión.

El mandato facultará al representante autorizado para que, además del proveedor o en su lugar, la Oficina de AI o las autoridades nacionales competentes se dirijan a él en todas las cuestiones relacionadas con el cumplimiento del presente Reglamento.

3. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor actúa de forma contraria a las obligaciones que le incumben en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la Oficina de AI de la terminación del mandato y de los motivos de la misma.

4. La obligación establecida en el presente artículo no se aplicará a los proveedores de modelos de IA de propósito general que se hagan accesibles al público en virtud de una licencia gratuita y de código abierto que permita el acceso, el uso, la modificación y la distribución del modelo, y cuyos parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, a menos que los modelos de IA de propósito general presenten riesgos sistémicos.

# Capítulo 3

# OBLIGACIONES PARA LOS PROVEEDORES DE MODELOS AI DE PROPÓSITO GENERAL CON RIESGO SISTÉMICO

*Artículo 52 quinquies*

**Obligaciones de los proveedores de modelos de IA de propósito general con riesgo sistémico**

1. Además de las obligaciones enumeradas en el artículo 52 quater, los proveedores de modelos de IA de propósito general con riesgo sistémico deberán:

(a) llevar a cabo la evaluación del modelo de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, incluida la realización y documentación de pruebas contradictorias del modelo con vistas a identificar y mitigar el riesgo sistémico;

(b) evaluar y mitigar los posibles riesgos sistémicos a escala de la Unión, incluidas sus fuentes, que puedan derivarse del desarrollo, la comercialización o el uso de modelos de IA de propósito general con riesgo sistémico;

(c) hacer un seguimiento, documentar y comunicar sin demora indebida a la Oficina de AI y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctivas para hacerles frente;

garantizar un nivel adecuado de protección de ciberseguridad para el modelo de IA de propósito general con riesgo sistémico y la infraestructura física del modelo.

2. Los proveedores de modelos de IA de propósito general con riesgo sistémico podrán basarse en códigos de prácticas en el sentido del artículo E para demostrar el cumplimiento de las obligaciones del apartado 1, hasta que se publique una norma armonizada. El cumplimiento de una norma armonizada europea otorga a los proveedores la presunción de conformidad. Los proveedores de modelos de IA de propósito general con riesgos sistémicos que no se adhieran a un código de buenas prácticas aprobado deberán demostrar medios alternativos adecuados de cumplimiento para su aprobación por la Comisión.

3. Toda información y documentación obtenida en virtud de lo dispuesto en el presente artículo, incluidos los secretos comerciales, se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 70.

*Artículo 52 sexies*

**Códigos de buenas prácticas**

1. La Oficina de AI fomentará y facilitará la elaboración de códigos de prácticas a escala de la Unión como elemento para contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta los planteamientos internacionales.

2. La Oficina de AI y el Consejo de Administración de AI procurarán garantizar que los códigos de buenas prácticas cubran, sin limitarse necesariamente a ello, las obligaciones previstas en los artículos 52 quater y 52 quinquies, incluidas las siguientes cuestiones:

(a) medios para garantizar que la información a que se refieren las letras a) y b) del artículo 52 quater se mantiene actualizada a la luz de la evolución del mercado y la tecnología, y el nivel de detalle adecuado para el resumen sobre el contenido utilizado para la formación;

(b) la identificación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluidas sus fuentes cuando proceda;

(c) las medidas, procedimientos y modalidades de evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación. La evaluación y la gestión de los riesgos sistémicos a escala de la Unión serán proporcionales a los riesgos, tomarán en consideración su gravedad y probabilidad y tendrán en cuenta los retos específicos de hacer frente a esos riesgos a la luz de las posibles formas en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA.

La Oficina de IA podrá invitar a los proveedores de modelos de IA de propósito general, así como a las autoridades nacionales competentes pertinentes, a participar en la elaboración de códigos de buenas prácticas. Las organizaciones de la sociedad civil, la industria, el mundo académico y otras partes interesadas pertinentes, como los proveedores posteriores y los expertos independientes, podrán apoyar el proceso.

3. La Oficina de AI y la Junta Directiva procurarán garantizar que los códigos de buenas prácticas establezcan claramente sus objetivos específicos y contengan compromisos o medidas, incluidos indicadores clave de rendimiento, según proceda, para garantizar la consecución de dichos objetivos y tengan debidamente en cuenta las necesidades e intereses de todas las partes interesadas, incluidas las personas afectadas, a escala de la Unión.

4. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de propósito general a participar en los códigos de buenas prácticas. En el caso de los proveedores de modelos de IA de propósito general que no presenten riesgos sistémicos, esta participación deberá limitarse a las obligaciones previstas en el apartado 2, letra a), del presente artículo, a menos que declaren explícitamente su interés por adherirse al código completo.

5. La Oficina de AI tratará de garantizar que los participantes en los códigos de buenas prácticas informen periódicamente a la Oficina de AI sobre la aplicación de los compromisos y las medidas adoptadas y sus resultados, incluidos los medidos en relación con los indicadores clave de rendimiento, según proceda. Los indicadores clave de resultados y los compromisos de información tendrán en cuenta las diferencias de tamaño y capacidad entre los distintos participantes.

6. La Oficina AI y el Consejo AI supervisarán y evaluarán periódicamente la consecución de los objetivos de los códigos de buenas prácticas por parte de los participantes y su contribución a la correcta aplicación del presente Reglamento. La Oficina AI y el Consejo AI evaluarán si los códigos de buenas prácticas cubren las obligaciones previstas en los artículos 52 quater y 52 quinquies, incluidas las cuestiones enumeradas en el apartado 2 del presente artículo, y supervisarán y evaluarán periódicamente la consecución de sus objetivos. Publicarán su evaluación de la adecuación de los códigos de buenas prácticas. La Comisión podrá decidir, mediante actos de ejecución, aprobar el código de buenas prácticas y darle una validez general en la Unión. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen establecido en el apartado 2 del artículo 74.

7. Cuando proceda, la Oficina de AI también fomentará y facilitará la revisión y adaptación de los códigos de buenas prácticas, en particular a la luz de las normas emergentes. La Oficina de AI colaborará en la evaluación de las normas disponibles.

8. Si, en el momento en que el Reglamento sea aplicable, no se puede ultimar un Código de buenas prácticas, o si la Oficina de AI considera que no es adecuado tras lo dispuesto en el apartado 7, la Comisión

podrá establecer, mediante actos de ejecución, normas comunes para la aplicación de las obligaciones previstas en los artículos 52 quater y 52 quinquies, incluidas las cuestiones contempladas en el apartado 2.

# TÍTULO V
# MEDIDAS DE APOYO A LA INNOVACIÓN

*Artículo 53*

**Cajas de arena reguladoras de la IA**

1. Los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio aislado de regulación de la IA a nivel nacional, que estará operativo 24 meses después de la entrada en vigor. Este sandbox también podrá establecerse conjuntamente con una o varias autoridades competentes de otros Estados miembros. La Comisión podrá proporcionar apoyo técnico, asesoramiento e instrumentos para la creación y el funcionamiento de los espacios aislados de regulación de la IA.

La obligación establecida en el párrafo anterior también puede cumplirse mediante la participación en un sandbox existente en la medida en que esta participación proporcione un nivel equivalente de cobertura nacional para los Estados miembros participantes.

1a.También podrán crearse otros espacios aislados de regulación de la IA a nivel regional o local o conjuntamente con las autoridades competentes de otros Estados miembros.

1 ter. El Supervisor Europeo de Protección de Datos también podrá establecer un espacio aislado de regulación de la IA para las instituciones, organismos y agencias de la UE y ejercer las funciones y tareas de las autoridades nacionales competentes de conformidad con el presente capítulo.

1 quáter. Los Estados miembros velarán por que las autoridades competentes a que se refieren los apartados 1 y 1 bis asignen recursos suficientes para cumplir el presente artículo de manera eficaz y oportuna. Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes del ecosistema de la IA.

El presente artículo no afectará a otros compartimentos estancos reguladores establecidos en virtud del Derecho nacional o de la Unión. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan esos otros compartimentos estancos y las autoridades nacionales competentes.

1d. Los entornos aislados de regulación de la IA establecidos en virtud del artículo 53, apartado 1, del presente Reglamento proporcionarán, de conformidad con los artículos 53 y 53 bis, un entorno controlado que fomente la innovación y facilite el desarrollo, la formación, las pruebas y la validación de sistemas de IA innovadores durante un tiempo limitado antes de su comercialización o puesta en servicio.

con arreglo a un plan específico de sandbox acordado entre los posibles proveedores y la autoridad competente. Estos entornos aislados reglamentarios pueden incluir pruebas en condiciones reales supervisadas en el entorno aislado.

1e. Las autoridades competentes proporcionarán, según proceda, orientación, supervisión y apoyo dentro del recinto de seguridad con vistas a identificar los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, los ensayos, las medidas de mitigación y su eficacia en relación con las obligaciones y los requisitos del presente Reglamento y, en su caso, de otra legislación de la Unión y de los Estados miembros supervisada dentro del recinto de seguridad.

1f.Las autoridades competentes proporcionarán a los proveedores y posibles proveedores orientación sobre las expectativas reglamentarias y sobre cómo cumplir los requisitos y obligaciones establecidos en el presente Reglamento.

A petición del proveedor o posible proveedor del sistema de IA, la autoridad competente facilitará una prueba escrita de las actividades realizadas con éxito en el espacio aislado. La autoridad competente facilitará asimismo un informe de salida en el que se detallen las actividades realizadas en el espacio aislado y los resultados y enseñanzas correspondientes. Los proveedores podrán utilizar dicha documentación para demostrar el cumplimiento del presente Reglamento a través del proceso de evaluación de la conformidad o de las actividades pertinentes de vigilancia del mercado. A este respecto, las autoridades de vigilancia del mercado y los organismos notificados tendrán positivamente en cuenta los informes de salida y las pruebas escritas facilitados por la autoridad nacional competente, con vistas a acelerar los procedimientos de evaluación de la conformidad en una medida razonable.

1 bis. Sin perjuicio de las disposiciones en materia de confidencialidad del artículo 70 y con el acuerdo del proveedor o posible proveedor del arenero, la Comisión Europea y la Junta Directiva estarán autorizadas a acceder a los informes de salida y los tendrán en cuenta, según proceda, en el ejercicio de sus funciones con arreglo al presente Reglamento. Si tanto el proveedor como el proveedor potencial y la autoridad nacional competente están explícitamente de acuerdo con ello, el informe de salida podrá ponerse a disposición del público a través de la plataforma única de información a que se refiere el presente artículo.

1g. La creación de espacios aislados de regulación de la IA tendrá por objeto contribuir a los siguientes objetivos:

(a) mejorar la seguridad jurídica para lograr el cumplimiento normativo del presente Reglamento o, en su caso, de otra legislación aplicable de la Unión y de los Estados miembros;

(b) apoyar el intercambio de buenas prácticas mediante la cooperación con las autoridades que participan en el espacio aislado de regulación de la IA;

(c) fomentar la innovación y la competitividad y facilitar el desarrollo de una IA

ecosistema;

(d) contribuir al aprendizaje normativo basado en pruebas;

(e) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los suministran pequeñas y medianas empresas (PYME), incluidas las empresas de nueva creación.

2. Las autoridades nacionales competentes velarán por que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o entren de otro modo en el ámbito de supervisión de otras autoridades nacionales o autoridades competentes que faciliten o apoyen el acceso a los datos, las autoridades nacionales de protección de datos y esas otras autoridades nacionales estén asociadas al funcionamiento del espacio aislado regulador de la IA y participen en la supervisión de esos aspectos en la medida de sus respectivas funciones y competencias, según proceda.

3. Los espacios aislados de regulación de la IA no afectarán a los poderes de supervisión y corrección de las autoridades competentes que supervisan los espacios aislados, incluso a nivel regional o local. Cualquier riesgo significativo para la salud y la seguridad y los derechos fundamentales que se detecte durante el desarrollo y las pruebas de dichos sistemas de IA dará lugar a una mitigación adecuada. Las autoridades nacionales competentes estarán facultadas para suspender temporal o permanentemente el proceso de ensayo o la participación en el espacio aislado si no es posible una mitigación eficaz, e informarán a la Oficina de la IA de tal decisión. Las autoridades nacionales competentes ejercerán sus facultades de supervisión dentro de los límites de la legislación pertinente, haciendo uso de sus facultades discrecionales cuando apliquen las disposiciones legales a un proyecto específico de sandbox de IA, con el objetivo de apoyar la innovación en IA en la Unión.

4. Los proveedores y posibles proveedores del espacio aislado de regulación de la IA seguirán siendo responsables, en virtud de la legislación aplicable de la Unión y de los Estados miembros en materia de responsabilidad, de cualquier daño causado a terceros como consecuencia de la experimentación que tenga lugar en el espacio aislado. No obstante, siempre que el proveedor o proveedores potenciales respeten el plan específico y las condiciones de su participación y sigan de buena fe las orientaciones dadas por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracción del presente Reglamento. En la medida en que otras autoridades competentes responsables de otra legislación de la Unión y de los Estados miembros hayan participado activamente en la supervisión del sistema de IA en el espacio aislado y hayan proporcionado orientaciones para su cumplimiento, no se impondrán multas administrativas en relación con dicha legislación.

4 ter. Los espacios aislados de regulación de la IA se diseñarán y aplicarán de forma que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.

Las autoridades nacionales competentes coordinarán sus actividades y cooperarán en el marco del Consejo.

5 bis. Las autoridades nacionales competentes informarán a la Oficina de Inteligencia Artificial y al Consejo de la creación de un espacio aislado y podrán solicitar apoyo y orientación. La Oficina de Inteligencia Artificial pondrá a disposición del público una lista de los entornos aislados de regulación previstos y existentes y la mantendrá actualizada con el fin de fomentar una mayor interacción en los entornos aislados de regulación y la cooperación transfronteriza.

5 ter.Las autoridades nacionales competentes presentarán a la Oficina de la IA y al Consejo informes anuales, comenzando un año después de la creación del compartimento estanco de regulación de la IA y posteriormente cada año hasta su finalización, así como un informe final. Dichos informes contendrán información sobre los avances y resultados de la aplicación de dichos compartimentos estancos, incluidas las mejores prácticas, los incidentes, las lecciones aprendidas y las recomendaciones sobre su configuración y, en su caso, sobre la aplicación y posible revisión del presente Reglamento, incluidos sus actos delegados y de ejecución, y demás legislación de la Unión supervisada dentro del compartimento estanco. Dichos informes anuales o resúmenes de los mismos se pondrán a disposición del público en línea. La Comisión tendrá en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones con arreglo al presente Reglamento.

5. La Comisión desarrollará una interfaz única y específica que contenga toda la información pertinente relacionada con los entornos aislados para permitir a las partes interesadas interactuar con los entornos aislados reguladores y plantear preguntas a las autoridades competentes, así como solicitar orientaciones no vinculantes sobre la conformidad de los productos, servicios y modelos de negocio innovadores que incorporen tecnologías de IA, de conformidad con el artículo 55, apartado 1, letra c). La Comisión se coordinará de forma proactiva con las autoridades nacionales competentes, cuando proceda.

*Artículo 53 bis*

**Modalidades y funcionamiento de los espacios aislados de regulación de la IA**

1. Para evitar la fragmentación en toda la Unión, la Comisión adoptará un acto de ejecución en el que se detallarán las modalidades de creación, desarrollo, aplicación, funcionamiento y supervisión de los espacios aislados de regulación de la IA. El acto de ejecución incluirá principios comunes sobre las siguientes cuestiones:

(a) elegibilidad y selección para participar en el espacio aislado de regulación de la IA;

(b) procedimiento para la solicitud, participación, supervisión, salida y finalización del espacio aislado de regulación de la IA, incluido el plan del espacio aislado y el

salir de informe;

(c) las condiciones aplicables a los participantes.

Los actos de ejecución garantizarán que:

(a) Los "areneros" reguladores están abiertos a cualquier proveedor potencial de un sistema de IA que cumpla los criterios de elegibilidad y selección. Los criterios de acceso al espacio aislado de regulación son transparentes y equitativos, y las autoridades competentes informan a los interesados de las condiciones de acceso.

a los solicitantes de su decisión en un plazo de 3 meses a partir de la solicitud;

(b) Los "sandboxes" reguladores permiten un acceso amplio e igualitario y se mantienen al día con la demanda de participación; los posibles proveedores también pueden presentar solicitudes en asociación con usuarios y otros terceros pertinentes;

(c) las modalidades y condiciones relativas a los compartimentos estancos de regulación apoyarán en la mayor medida posible la flexibilidad de las autoridades nacionales competentes para establecer y gestionar sus compartimentos estancos de regulación de la IA;

(d) el acceso a los espacios aislados de regulación de la IA es gratuito para las PYME y las empresas de nueva creación, sin perjuicio de los costes excepcionales que las autoridades nacionales competentes puedan recuperar de manera justa y proporcionada;

(e) facilitan a los posibles proveedores, mediante los resultados de aprendizaje de los entornos aislados, la realización de las obligaciones de evaluación de la conformidad del presente Reglamento o

la aplicación voluntaria de los códigos de conducta contemplados en el artículo 69;

(f) los espacios aislados reglamentarios facilitan la participación de otros agentes pertinentes del ecosistema de la IA, como los organismos notificados y las organizaciones de normalización

(PYME, start-ups, empresas, innovadores, instalaciones de ensayo y experimentación, laboratorios experimentación, laboratorios de investigación y experimentación y centros de innovación digital, centros de excelencia, investigadores individuales), con el fin de permitir y facilitar la cooperación con el sector público y privado;

(g) los procedimientos, procesos y requisitos administrativos para la solicitud, selección, participación y salida del sandbox sean sencillos, fácilmente inteligibles, claramente

comunicados para facilitar la participación de las PYME y las empresas de nueva creación con capacidades jurídicas y administrativas limitadas y se racionalicen en toda la Unión, con el fin de evitar la fragmentación y que la participación en un sandbox reglamentario por un Estado miembro o por el SEPD se reconozca mutua y uniformemente y produzca los mismos efectos jurídicos en toda la Unión. y tenga los mismos efectos jurídicos en toda la Unión;

(h) la participación en el espacio aislado de regulación de la IA se limita a un período

en función de la complejidad y envergadura del proyecto. Este plazo podrá ser prorrogado por la autoridad nacional competente;

(i) los "sandboxes" facilitarán el desarrollo de herramientas e infraestructuras para probar, comparar, evaluar y explicar las dimensiones de la IA sistemasrelevantes para el aprendizaje normativo, como la precisión, la solidez y la ciberseguridad, así como medidas para mitigar los riesgos para la y la sociedad en general.

3. Los posibles proveedores de los espacios aislados, en particular las PYME y las empresas de nueva creación, serán dirigidos, en su caso, a los servicios previos al despliegue, como la orientación sobre la aplicación del presente Reglamento, a otros servicios de valor añadido, como la ayuda con los documentos de normalización y la certificación, las instalaciones de ensayo y experimentación, los centros digitales y los centros de excelencia.

4. Cuando las autoridades nacionales competentes consideren la posibilidad de autorizar ensayos en condiciones reales supervisados en el marco de un espacio aislado de regulación de la IA establecido con arreglo al presente artículo, acordarán específicamente con los participantes las condiciones de dichos ensayos y, en particular, las salvaguardias adecuadas con vistas a proteger los derechos fundamentales, la salud y la seguridad. Cuando proceda, cooperarán con otras autoridades nacionales competentes con vistas a garantizar prácticas coherentes en toda la Unión.

*Artículo 54*

**Tratamiento adicional de datos personales para el desarrollo de determinados sistemas de IA de interés público en el espacio aislado de regulación de la IA**

1. En el espacio aislado de regulación de la IA, los datos personales recogidos legalmente para otros fines podrán tratarse únicamente con el fin de desarrollar, formar y probar determinados sistemas de IA en el espacio aislado cuando se cumplan todas las condiciones siguientes:

(a) Los sistemas de IA serán desarrollados para salvaguardar intereses públicos sustanciales por una autoridad pública u otra persona física o jurídica de Derecho público o de Derecho privado y en uno o varios de los siguientes ámbitos:

(ii) seguridad pública y salud pública, incluida la detección de enfermedades, la prevención del diagnóstico, el control y el tratamiento y la mejora de los sistemas de asistencia sanitaria;

un alto nivel de protección y mejora de la calidad del medio ambiente, protección de la biodiversidad, contaminación, así como transición ecológica, mitigación del cambio climático y adaptación al mismo;

(iiia) sostenibilidad energética;

(iiib) seguridad y resistencia de los sistemas de transporte y movilidad, infraestructuras críticas y redes;

(iiic) eficiencia y calidad de la administración pública y los servicios públicos;

(b) los datos tratados son necesarios para cumplir uno o varios de los requisitos contemplados en el capítulo 2 del título III, cuando dichos requisitos no puedan cumplirse eficazmente mediante el tratamiento de datos anónimos, sintéticos u otros datos de carácter no personal;

(c) existen mecanismos de supervisión eficaces para identificar si durante la experimentación del sandbox pueden surgir riesgos elevados para los derechos y libertades de los interesados, a los que se hace referencia en el artículo 35 del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725, así como mecanismo de respuesta para mitigar rápidamente esos riesgos y, en su caso, detener el tratamiento;

(d) los datos personales que vayan a tratarse en el contexto del sandbox se encuentren en un entorno de tratamiento de datos funcionalmente separado, aislado y protegido, bajo el control del futuro proveedor, y sólo las personas autorizadas tengan acceso a dichos datos;

(e) Los proveedores sólo pueden compartir los datos recogidos originalmente de conformidad con la legislación de protección de datos de la UE. Los datos personales creados en el espacio aislado no pueden compartirse fuera de él;

(f) cualquier tratamiento de datos personales en el contexto del sandbox no dé lugar a medidas o decisiones que afecten a los interesados ni afecte a la aplicación de sus derechos establecidos en el Derecho de la Unión en materia de protección de datos personales;

(g) todos los datos personales tratados en el contexto del sandbox se protejan mediante medidas técnicas y organizativas adecuadas y se supriman una vez finalizada la participación en el sandbox o cuando los datos personales hayan alcanzado el final de su período de conservación;

(h) los registros del tratamiento de datos personales en el contexto del sandbox se conservan mientras dure la participación en el sandbox, salvo disposición en contrario del Derecho de la Unión o nacional;

En el Anexo IV de la documentación técnica se incluye una descripción completa y detallada del proceso y la justificación de la formación, las pruebas y la validación del sistema de IA, junto con los resultados de las pruebas;

(i) un breve resumen del proyecto de IA desarrollado en el espacio aislado, sus objetivos y resultados esperados publicados en el sitio web de las autoridades competentes. Esta obligación no cubrirá los datos operativos sensibles en relación con las actividades de las autoridades policiales, de control de fronteras, de inmigración o de asilo.

1 bis. Con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención de amenazas para la seguridad pública, bajo el control y la responsabilidad de las autoridades policiales, el tratamiento de datos personales en los entornos aislados de regulación de la IA se basará en la legislación específica de un Estado miembro o de la Unión y estará sujeto a las mismas condiciones acumulativas que se mencionan en el apartado 1.

2. El apartado 1 se entenderá sin perjuicio de la legislación de la Unión o de los Estados miembros que excluya el tratamiento para fines distintos de los mencionados explícitamente en dicha legislación, así como de la legislación de la Unión o de los Estados miembros que establezca la base para el tratamiento de datos personales que sea necesario a efectos de desarrollo, prueba y formación de sistemas innovadores de IA o cualquier otra base jurídica, de conformidad con el Derecho de la Unión en materia de protección de datos personales.

*Artículo 54 bis*

**Pruebas de sistemas de IA de alto riesgo en condiciones del mundo real fuera de los "cajones de arena" reguladores de la IA.**

1. Los proveedores o posibles proveedores de sistemas de IA de alto riesgo enumerados en el anexo III podrán realizar pruebas de sistemas de IA en condiciones del mundo real fuera de los entornos aislados reguladores de la IA, de conformidad con las disposiciones del presente artículo y el plan de pruebas en condiciones reales a que se refiere el presente artículo, sin perjuicio de las prohibiciones establecidas en el artículo 5.

Los elementos detallados del plan de pruebas en condiciones reales se especificarán en actos de ejecución adoptados por la Comisión de conformidad con el procedimiento de examen contemplado en el artículo 74, apartado 2.

Esta disposición se entenderá sin perjuicio de la legislación de la Unión o nacional para la realización de pruebas en condiciones reales de sistemas de IA de alto riesgo relacionados con productos cubiertos por la legislación enumerada en el anexo II.

Los proveedores o posibles proveedores podrán realizar pruebas de los sistemas de IA de alto riesgo a que se refiere el anexo III en condiciones reales en cualquier momento antes de la comercialización o puesta en servicio del sistema de IA por sí mismos o en asociación con uno o varios posibles implantadores.

2. Las pruebas de sistemas de IA de alto riesgo en condiciones del mundo real con arreglo al presente artículo se realizarán sin perjuicio de la revisión ética que pueda exigir la legislación nacional o de la Unión.

3. Los proveedores o posibles proveedores sólo podrán realizar las pruebas en condiciones reales cuando se cumplan todas las condiciones siguientes:

(a) el proveedor o posible proveedor haya elaborado un plan de pruebas en condiciones reales y lo haya presentado a la autoridad de vigilancia del mercado del Estado o Estados miembros en los que vayan a realizarse las pruebas en condiciones reales;

(b) la autoridad de vigilancia del mercado del Estado o Estados miembros en los que vayan a realizarse los ensayos en condiciones reales haya aprobado los ensayos en condiciones reales y el plan de ensayos en condiciones reales. En caso de que la autoridad de vigilancia del mercado de dicho Estado miembro no haya respondido en un plazo de 30 días, los ensayos en condiciones reales y el plan de ensayos en condiciones reales se entenderán aprobados. En los casos en que la legislación nacional no prevea una aprobación tácita, las pruebas en condiciones reales estarán sujetas a una autorización;

(c) el proveedor o posible proveedor, con excepción de los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 y 7, en los ámbitos de la aplicación de la ley, la migración, el asilo y la gestión del control fronterizo, y los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, haya registrado los ensayos en condiciones reales en la parte no pública de la base de datos de la UE a que se refiere el artículo 60, apartado 3, con un número de identificación único para toda la Unión y la información especificada en el anexo VIII bis;

(d) el proveedor o posible proveedor que realice las pruebas en condiciones reales esté establecido en la Unión o haya designado a un representante legal que esté establecido en la Unión;

(e) los datos recogidos y tratados a efectos de las pruebas en condiciones reales sólo se transferirán a terceros países fuera de la Unión siempre que se apliquen las salvaguardias adecuadas y aplicables en virtud del Derecho de la Unión;

(f) las pruebas en condiciones reales no duren más de lo necesario para alcanzar sus objetivos y, en cualquier caso, no superen los 6 meses, prorrogables por un

cantidad adicional de 6 meses, previa notificación por parte del proveedor a la autoridad de vigilancia del mercado, acompañada de una explicación sobre la necesidad de dicha prórroga;

(g) se proteja adecuadamente a las personas pertenecientes a grupos vulnerables por su edad o discapacidad física o mental;

(h) cuando un proveedor o posible proveedor organice los ensayos en condiciones reales en cooperación con uno o varios posibles implantadores, estos últimos hayan sido informados de todos los aspectos de los ensayos que sean pertinentes para su decisión de participar y hayan recibido las instrucciones pertinentes sobre cómo utilizar el sistema de IA a que se refiere el artículo 13; el proveedor o posible proveedor y el implantador o implantadores celebrarán un acuerdo en el que se especifiquen sus funciones y responsabilidades con vistas a garantizar el cumplimiento de las disposiciones relativas a los ensayos en condiciones reales con arreglo al presente Reglamento y demás legislación aplicable de la Unión y de los Estados miembros;

(i) los sujetos de las pruebas en condiciones del mundo real hayan dado su consentimiento informado de conformidad con el artículo 54 ter, o en el caso de las fuerzas y cuerpos de seguridad, cuando la solicitud del consentimiento informado impidiera la realización de las pruebas del sistema de IA, las propias pruebas y el resultado de las pruebas en condiciones del mundo real no tendrán ningún efecto negativo sobre el sujeto y sus datos personales se suprimirán una vez realizadas las pruebas;

(j) las pruebas en condiciones reales sean supervisadas de forma efectiva por el proveedor o posible proveedor y el desplegador o desplegadores con personas debidamente cualificadas en el ámbito pertinente y que tengan la capacidad, la formación y la autoridad necesarias para desempeñar sus tareas;

(k) las predicciones, recomendaciones o decisiones del sistema de IA pueden ser efectivamente anuladas e ignoradas.

5Cualquier sujeto de las pruebas en condiciones reales, o su representante legalmente designado, según proceda, podrá, sin que ello suponga perjuicio alguno y sin tener que aportar justificación alguna, retirarse de las pruebas en cualquier momento revocando su consentimiento informado y solicitar la supresión inmediata y permanente de sus datos personales. La revocación del consentimiento informado no afectará a las actividades ya realizadas.

5 bis.De conformidad con el artículo 63 bis, los Estados miembros conferirán a sus autoridades de vigilancia del mercado la facultad de exigir información a los proveedores y posibles proveedores, de realizar inspecciones a distancia o in situ sin previo aviso y de efectuar controles de la

desarrollo de las pruebas en condiciones reales y los productos relacionados. Las autoridades de vigilancia del mercado utilizarán estas competencias para garantizar un desarrollo seguro de estos ensayos.

5. Cualquier incidente grave detectado en el transcurso de los ensayos en condiciones reales se notificará a la autoridad nacional de vigilancia del mercado de conformidad con el artículo 62 del presente Reglamento. El proveedor o posible proveedor adoptará medidas paliativas inmediatas o, en su defecto, suspenderá los ensayos en condiciones reales hasta que se lleve a cabo dicha paliación o, de lo contrario, pondrá fin a los mismos. El proveedor o posible proveedor establecerá un procedimiento para la rápida recuperación del sistema de IA tras la finalización de los ensayos en condiciones reales.

6. Los proveedores o posibles proveedores notificarán a la autoridad nacional de vigilancia del mercado del Estado o Estados miembros en los que vayan a realizarse las pruebas en condiciones reales la suspensión o finalización de las pruebas en condiciones reales y los resultados finales.

7. El proveedor y el posible proveedor serán responsables, en virtud de la legislación aplicable en materia de responsabilidad de la Unión y de los Estados miembros, de cualquier daño causado en el transcurso de su participación en las pruebas en condiciones reales.

*Artículo 54 ter*

**Consentimiento informado para participar en pruebas en condiciones del mundo real fuera de los espacios aislados de regulación de la IA.**

1. A efectos de la realización de pruebas en condiciones reales con arreglo al artículo 54 bis, el consentimiento informado deberá ser otorgado libremente por el sujeto de la prueba antes de su participación en la misma y después de haber sido debidamente informado con información concisa, clara, pertinente y comprensible sobre:

(i) la naturaleza y los objetivos de las pruebas en condiciones reales y los posibles inconvenientes que pueda acarrear su participación;

(ii) las condiciones en las que se realizarán las pruebas en condiciones reales, incluida la duración prevista de la participación del sujeto;

(iii) los derechos y garantías del sujeto en relación con su participación, en particular su derecho a negarse a participar y a retirarse de las pruebas en el mundo real condiciones en cualquier momento sin ningún perjuicio resultante y sin tener que aportar justificación alguna;

las modalidades para solicitar la anulación o el incumplimiento de las predicciones, recomendaciones o decisiones del sistema de IA;

(iv) el número único de identificación a escala de la Unión del ensayo en condiciones reales, de conformidad con el artículo 54 bis, apartado 4 quater, y los datos de contacto del proveedor o de su representante legal del que pueda obtenerse más información.

2El consentimiento informado se fechará y documentará y se entregará una copia al sujeto o a su representante legal.

*Artículo 55*

**Medidas para proveedores e implantadores, en particular las PYME, incluidas las empresas de nueva creación**

1. Los Estados miembros emprenderán las siguientes acciones:

(a) proporcionará a las PYME, incluidas las de nueva creación, que tengan un domicilio social o una sucursal en la Unión, acceso prioritario a los entornos aislados de regulación de la IA, en la medida en que cumplan las condiciones de admisibilidad y los criterios de selección. El acceso prioritario no impedirá que otras PYME, incluidas las de nueva creación, distintas de las mencionadas en el párrafo primero, accedan al arenero regulador de la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección;

(b) organizar actividades específicas de sensibilización y formación sobre la aplicación del presente Reglamento adaptadas a las necesidades de las PYME, incluidas las empresas de nueva creación, los usuarios y, en su caso, las autoridades públicas locales;

(c) utilizar los canales específicos existentes y, en su caso, establecer otros nuevos para la comunicación con las PYME, incluidas las empresas de nueva creación, los usuarios, otros innovadores y, cuando proceda, las autoridades públicas locales, a fin de proporcionar asesoramiento y responder a las preguntas sobre la aplicación del presente Reglamento, incluso en lo que se refiere a la participación en los espacios aislados de regulación de la IA;

(c bis) facilitar la participación de las PYME y otras partes interesadas en el proceso de desarrollo de la normalización.

2. Se tendrán en cuenta los intereses y necesidades específicos de las PYME proveedoras, incluidas las de nueva creación, a la hora de fijar las tasas para la evaluación de la conformidad con arreglo al artículo 43, reduciendo dichas tasas proporcionalmente a su tamaño, tamaño de mercado y otros indicadores pertinentes.

2a. La Oficina de AI emprenderá las siguientes acciones:

a petición del Consejo de AI, proporcionar plantillas normalizadas para los ámbitos cubiertos por el presente Reglamento;

(a) desarrollar y mantener una plataforma de información única que proporcione información fácil de usar en relación con este Reglamento para todos los operadores de la Unión;

(b) organizar campañas de comunicación adecuadas para dar a conocer las obligaciones derivadas del presente Reglamento;

(c) evaluar y promover la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

*Artículo 55 bis*

**Excepciones para operadores específicos**

2 ter. Las microempresas, tal como se definen en el apartado 3 del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión sobre la definición de microempresas, pequeñas y medianas empresas, siempre que dichas empresas no tengan empresas asociadas o empresas vinculadas, tal como se definen en el artículo 3 del mismo anexo, podrán cumplir determinados elementos del sistema de gestión de la calidad exigido en el artículo 17 del presente Reglamento de forma simplificada. A tal fin, la Comisión elaborará directrices sobre los elementos del sistema de gestión de la calidad que podrán cumplirse de forma simplificada teniendo en cuenta las necesidades de las microempresas sin que ello afecte al nivel de protección y a la necesidad de cumplir los requisitos de los sistemas de IA de alto riesgo.

2 quater. El apartado 1 no se interpretará en el sentido de que exime a dichos operadores del cumplimiento de cualesquiera otros requisitos y obligaciones establecidos en el presente Reglamento, incluidos los establecidos en los artículos 9, 10, 11, 12, 13, 14, 15, 61 y 62.

**TÍTULO VI GOBERNANZA**

*Artículo 55 ter*

**Gobernanza a escala de la Unión**

1. La Comisión desarrollará los conocimientos y capacidades de la Unión en el ámbito de la inteligencia artificial. A tal fin, la Comisión ha creado la Oficina Europea de Inteligencia Artificial mediante la Decisión [...].

2. Los Estados miembros facilitarán las tareas encomendadas a la Oficina de AI, tal y como se refleja en el presente Reglamento.

# Capítulo 1

# CONSEJO EUROPEO DE INTELIGENCIA ARTIFICIAL

*Artículo 56*

**Creación y estructura del Consejo Europeo de Inteligencia Artificial**

1. Se crea una "Junta Europea de Inteligencia Artificial" (la "Junta").

2. El Consejo estará compuesto por un representante de cada Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Oficina de AI también asistirá a las reuniones del Consejo sin participar en las votaciones. La Junta podrá invitar a las reuniones, caso por caso, a otras autoridades, organismos o expertos nacionales y de la Unión, cuando las cuestiones debatidas sean pertinentes para ellos.

2 bis. Cada representante será designado por su Estado miembro por un período de 3 años, renovable una vez.

2b.Los Estados miembros velarán por que sus representantes en el Consejo:

(a) dispongan de las competencias y poderes pertinentes en su Estado miembro para contribuir activamente a la realización de las tareas del Consejo contempladas en el artículo 58;

(b) se designan como punto de contacto único ante el Consejo y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;

están facultadas para facilitar la coherencia y la coordinación entre las autoridades nacionales competentes de su Estado miembro por lo que se refiere a la aplicación de la presente Directiva.

Reglamento, incluso mediante la recopilación de datos e información pertinentes para el cumplimiento de sus funciones en el Consejo.

3. Los representantes designados de los Estados miembros aprobarán el reglamento interno del Consejo por mayoría de dos tercios. El reglamento interno establecerá, en particular, los procedimientos para el proceso de selección, la duración del mandato y las especificaciones de las tareas del Presidente, las modalidades de votación y la organización de las actividades de la Junta y sus subgrupos.

3 bis.El Consejo creará dos subgrupos permanentes para proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y las autoridades notificantes sobre cuestiones relacionadas con la vigilancia del mercado y los organismos notificados, respectivamente.

El subgrupo permanente de vigilancia del mercado debe actuar como Grupo de Cooperación Administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020.

El Consejo podrá crear otros subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas. Cuando proceda, podrá invitarse a representantes del foro consultivo contemplado en el artículo 58 bis a dichos subgrupos o a reuniones específicas de los mismos en calidad de observadores.

3b.El Consejo se organizará y funcionará de forma que se salvaguarde la objetividad e imparcialidad de sus actividades.

4. El Consejo estará presidido por uno de los representantes de los Estados miembros. La Oficina Europea de Armonización se encargará de la secretaría del Comité, convocará las reuniones a petición del presidente y preparará el orden del día de conformidad con las tareas del Comité en virtud del presente Reglamento y de su reglamento interno.

Artículo 58

**Tareas del Consejo**

La Junta asesorará y asistirá a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del presente Reglamento. A tal fin, la Junta podrá, en particular:

(a) contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del presente Reglamento y, en cooperación y previo acuerdo de las autoridades de vigilancia del mercado interesadas, apoyar las actividades conjuntas de las autoridades de vigilancia del mercado a que se refiere el artículo 63, apartado 7 bis;

(b) recopilar y compartir conocimientos técnicos y reglamentarios y buenas prácticas entre los Estados miembros;

(c) asesorar en la aplicación del presente Reglamento, en particular por lo que respecta a la aplicación de las normas sobre modelos de IA de propósito general;

(d) contribuir a la armonización de las prácticas administrativas en los Estados miembros, incluso en relación con la excepción de los procedimientos de evaluación de la conformidad a que se refiere el artículo 47, el funcionamiento de los "cajones de arena" reglamentarios y los ensayos en condiciones reales a que se refieren los artículos 53, 54 y 54 bis;

(e) a petición de la Comisión o por iniciativa propia, emitir recomendaciones y dictámenes escritos sobre cualquier asunto pertinente relacionado con la ejecución del presente Reglamento y con su aplicación coherente y eficaz, incluyendo:

(i) sobre el desarrollo y la aplicación de códigos de conducta y códigos de prácticas en virtud del presente Reglamento, así como de las directrices de la Comisión;

(ii) la evaluación y revisión del presente Reglamento con arreglo al artículo 84, incluido lo relativo a los informes sobre incidentes graves a que se refiere el artículo 62 y al funcionamiento de la base de datos a que se refiere el artículo 60, la preparación de los actos delegados o de ejecución, y las posibles adaptaciones del presente Reglamento a los actos jurídicos enumerados en el anexo II;

(iii) sobre especificaciones técnicas o normas existentes en relación con los requisitos establecidos en el capítulo 2 del título III;

(iv) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41;

tendencias, como la competitividad global europea en inteligencia artificial, la adopción de la inteligencia artificial en la Unión y el desarrollo de competencias digitales;

(vía) tendencias sobre la evolución de la tipología de las cadenas de valor de la IA, en particular sobre las implicaciones resultantes en términos de responsabilidad;

(v) sobre la posible necesidad de modificar el anexo III de conformidad con el artículo 7 y sobre la posible necesidad de revisar el artículo 5 de conformidad con el artículo 84, teniendo en cuenta las pruebas pertinentes disponibles y los últimos avances tecnológicos;

(f) apoyar a la Comisión en la promoción de la alfabetización en IA, la concienciación pública y la comprensión de los beneficios, riesgos, salvaguardias y derechos y obligaciones en relación con el uso de los sistemas de IA;

(g) facilitar el desarrollo de criterios comunes y una comprensión compartida entre los operadores del mercado y las autoridades competentes de los conceptos pertinentes previstos en el presente Reglamento, incluso contribuyendo al desarrollo de índices de referencia;

(h) cooperar, según proceda, con otras instituciones, órganos y organismos de la Unión, así como con los grupos y redes de expertos pertinentes de la Unión, en particular en los ámbitos de la seguridad de los productos, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, la protección de los consumidores y la protección de los datos y los derechos fundamentales;

(i) contribuir a la cooperación efectiva con las autoridades competentes de terceros países y con las organizaciones internacionales;

(j) asistir a las autoridades nacionales competentes y a la Comisión en el desarrollo de los conocimientos organizativos y técnicos necesarios para la aplicación del presente Reglamento, en particular contribuyendo a la evaluación de las necesidades de formación del personal de los Estados miembros que participe en la aplicación del presente Reglamento;

(j1) ayudar a la Oficina de la IA a apoyar a las autoridades nacionales competentes en el establecimiento y desarrollo de los compartimentos estancos de regulación y facilitar la cooperación y el intercambio de información entre los compartimentos estancos de regulación;

(k) Contribuir a la elaboración de documentos de orientación y prestar el asesoramiento pertinente;

(l) asesorar a la Comisión en relación con asuntos internacionales sobre inteligencia artificial;

proporcionar dictámenes a la Comisión sobre las descripciones cualificadas relativas a los modelos de IA de uso general;

(m) recibir dictámenes de los Estados miembros sobre las descripciones cualificadas relativas a los modelos de IA de propósito general y sobre las experiencias y prácticas nacionales en materia de supervisión y aplicación de los sistemas de IA, en particular los sistemas que integran los modelos de IA de propósito general.

*Artículo 58 bis*

**Foro consultivo**

1. Se creará un foro consultivo para asesorar y proporcionar conocimientos técnicos a la Junta y a la Comisión con el fin de contribuir a sus tareas en virtud del presente Reglamento.

2. Los miembros del foro consultivo representarán una selección equilibrada de las partes interesadas, incluida la industria, las nuevas empresas, las PYME, la sociedad civil y el mundo académico. La composición del foro consultivo será equilibrada en lo que respecta a los intereses comerciales y no comerciales y, dentro de la categoría de intereses comerciales, en lo que respecta a las PYME y otras empresas.

3. La Comisión designará a los miembros del foro consultivo, de acuerdo con los criterios establecidos en el apartado anterior, entre las partes interesadas con experiencia reconocida en el ámbito de la IA.

4. La duración del mandato de los miembros del foro consultivo será de dos años, prorrogable hasta un máximo de cuatro años.

5. La Agencia de los Derechos Fundamentales, la Agencia de Ciberseguridad de la Unión Europea, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicación (ETSI) serán miembros permanentes del foro consultivo.

6. El Foro consultivo establecerá su reglamento interno. Elegirá dos copresidentes entre sus miembros, de conformidad con los criterios establecidos en el apartado 2. El mandato de los copresidentes será de dos años, renovable una vez. El mandato de los copresidentes será de dos años, renovable una sola vez.

7. El foro consultivo celebrará reuniones al menos dos veces al año. El foro consultivo podrá invitar a sus reuniones a expertos y otras partes interesadas.

8. En el desempeño de su función, tal como se establece en el apartado 1, el foro consultivo podrá elaborar dictámenes, recomendaciones y contribuciones escritas a petición del Consejo o de la Comisión.

El Foro Consultivo podrá crear subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento.

9. El foro consultivo elaborará un informe anual de sus actividades. Dicho informe se pondrá a disposición del público.

## Capítulo 1 bis

## PANEL CIENTÍFICO DE EXPERTOS INDEPENDIENTES

*Artículo 58 ter*

**Comité científico de expertos independientes**

1. La Comisión adoptará, mediante un acto de ejecución, disposiciones relativas a la creación de un grupo científico de expertos independientes ("el grupo científico") destinado a apoyar las actividades de ejecución en virtud del presente Reglamento. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

2. El comité científico estará compuesto por expertos seleccionados por la Comisión sobre la base de los conocimientos científicos o técnicos actualizados en el ámbito de la inteligencia artificial necesarios para las tareas establecidas en el apartado 3, y deberá poder demostrar que cumple todas las condiciones siguientes:

(a) experiencia y competencia particulares y conocimientos científicos o técnicos en el ámbito de la inteligencia artificial;

(b) independencia de cualquier proveedor de sistemas de IA o de modelos o sistemas de IA de propósito general;

(c) capacidad para llevar a cabo actividades con diligencia, precisión y objetividad.

La Comisión, en consulta con la Junta Directiva de AI, determinará el número de expertos del grupo en función de las necesidades y garantizará una representación geográfica y de género equitativa.

3. El panel científico asesorará y apoyará a la Oficina Europea de AI, en particular en lo que respecta a las siguientes tareas:

(a) apoyar la aplicación y el cumplimiento del presente Reglamento en lo que respecta a los modelos y sistemas de IA de propósito general, en particular mediante

alertar a la Oficina de Inteligencia Artificial de posibles riesgos sistémicos a nivel de la Unión de modelos de IA de propósito general, de conformidad con el artículo 68 nonies [*Alertas de riesgos sistémicos*

*por el panel científico*];

(i) Contribuir al desarrollo de herramientas y metodologías para evaluar las capacidades de los modelos y sistemas de IA de propósito general, incluso mediante evaluaciones comparativas;

(ii) asesorar sobre la clasificación de los modelos de IA de propósito general con riesgo sistémico;

(iii) asesorar sobre la clasificación de los distintos modelos y sistemas de IA de propósito general;

(iv) contribuir al desarrollo de herramientas y plantillas;

(b) apoyar la labor de las autoridades de vigilancia del mercado, a petición de éstas;

(c) apoyar las actividades transfronterizas de vigilancia del mercado a que se refiere el artículo 63, apartado 7 bis, sin perjuicio de las competencias de las autoridades de vigilancia del mercado;

(d) apoyar a la Oficina de AI en el desempeño de sus funciones en el contexto de la cláusula de salvaguardia con arreglo al artículo 66.

4. Los expertos desempeñarán sus tareas con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el desempeño de sus tareas y actividades. No solicitarán ni aceptarán instrucciones de nadie en el ejercicio de sus funciones con arreglo al apartado 3. Cada experto elaborará una declaración de intereses, que se hará pública. La Oficina de AI establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.

5. El acto de ejecución a que se refiere el apartado 1 incluirá disposiciones sobre las condiciones, el procedimiento y las modalidades para que la comisión técnica científica y sus miembros emitan alertas y soliciten la asistencia de la Oficina de la IA para el desempeño de sus tareas.

*Artículo 58 quater*

**Acceso de los Estados miembros a la reserva de expertos**

1. Los Estados miembros podrán recurrir a los expertos de la comisión técnica científica para que les apoyen en sus actividades de aplicación del presente Reglamento.

Podrá exigirse a los Estados miembros el pago de tasas por el asesoramiento y la asistencia de los expertos. La estructura y el nivel de las tasas, así como la escala y la estructura de los costes recuperables se establecerán en el acto de ejecución a que se refiere el artículo 58 ter, apartado 1, teniendo en cuenta los objetivos de la aplicación adecuada del presente Reglamento, la rentabilidad y la necesidad de garantizar un acceso efectivo a los expertos por parte de todos los Estados miembros.

2. La Comisión facilitará el acceso oportuno a los expertos por parte de los Estados miembros, según sea necesario, y velará por que la combinación de actividades de apoyo llevadas a cabo por la IA de la UE en apoyo de las pruebas con arreglo al artículo 68 bis y los expertos con arreglo al presente artículo se organice de manera eficiente y aporte el mejor valor añadido posible.

# Capítulo 2
# AUTORIDADES NACIONALES COMPETENTES

*Artículo 59*

**Designación de autoridades nacionales competentes y ventanilla única**

2. Cada Estado miembro establecerá o designará al menos una autoridad notificante y una autoridad de vigilancia del mercado a efectos del presente Reglamento como autoridades nacionales competentes. Estas autoridades nacionales competentes ejercerán sus competencias con independencia, imparcialidad y neutralidad, a fin de salvaguardar los principios de objetividad de sus actividades y funciones y garantizar la aplicación y ejecución del presente Reglamento. Los miembros de estas autoridades se abstendrán de toda acción incompatible con sus funciones. Siempre que se respeten dichos principios, tales actividades y tareas podrán ser desempeñadas por una o varias autoridades designadas, en función de las necesidades organizativas del Estado miembro.

3. Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. Los Estados miembros pondrán a disposición del público información sobre la forma de ponerse en contacto con las autoridades competentes y la ventanilla única, a través de medios de comunicación electrónica, a más tardar el ... [12 meses después de la fecha de entrada en vigor del presente Reglamento]. Los Estados miembros designarán a una autoridad de vigilancia del mercado para que actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad del punto de contacto único. La Comisión pondrá a disposición del público una lista de los puntos de contacto únicos.

Los Estados miembros velarán por que la autoridad nacional competente disponga de los recursos técnicos, financieros y humanos adecuados, así como de la infraestructura necesaria para desempeñar eficazmente sus funciones con arreglo al presente Reglamento. En particular, la autoridad nacional competente dispondrá permanentemente de un número suficiente de personal cuyas competencias y conocimientos especializados incluirán una comprensión profunda de las tecnologías de inteligencia artificial, los datos y la informática de datos, la protección de datos personales, la ciberseguridad, los derechos fundamentales, los riesgos para la salud y la seguridad y el conocimiento de las normas y los requisitos jurídicos existentes. Los Estados miembros evaluarán y, si lo consideran necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.

4 bis.Las autoridades nacionales competentes deberán satisfacer un nivel adecuado de medidas de ciberseguridad.

4c. En el desempeño de sus funciones, las autoridades nacionales competentes actuarán respetando las obligaciones de confidencialidad establecidas en el artículo 70.

4. A más tardar un año después de la entrada en vigor del presente Reglamento y, posteriormente, una vez cada dos años, los Estados miembros informarán a la Comisión sobre la situación de los recursos financieros y humanos de las autoridades nacionales competentes con una evaluación de su adecuación. La Comisión transmitirá esa información a la Junta para su debate y posibles recomendaciones.

5. La Comisión facilitará el intercambio de experiencias entre las autoridades nacionales competentes.

6. Las autoridades nacionales competentes podrán proporcionar orientación y asesoramiento sobre la aplicación del presente Reglamento, en particular a las PYME, incluidas las de nueva creación, teniendo en cuenta la orientación y el asesoramiento de la Junta y de la Comisión, según proceda. Siempre que las autoridades nacionales competentes tengan la intención de proporcionar orientación y asesoramiento con respecto a un sistema de IA en ámbitos cubiertos por otra legislación de la Unión, se consultará a las autoridades nacionales competentes en virtud de dicha legislación de la Unión, según proceda.

7. Cuando las instituciones, agencias y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como autoridad competente para su supervisión.

TÍTULO VII

# BASE DE DATOS DE LA UE PARA LOS SISTEMAS DE AI DE ALTO RIESGO ENUMERADOS EN EL ANEXO III

*Artículo 60*

**Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el anexo III**

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contenga la información a que se refieren los apartados 2 y 2 bis relativa a los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, que estén registrados de conformidad con los artículos 51 y 54 bis. Al establecer las especificaciones funcionales de dicha base de datos, la Comisión consultará a los expertos pertinentes, y al actualizar las especificaciones funcionales de dicha base de datos, la Comisión consultará al Consejo de IA.

2. Los datos enumerados en el anexo VIII, sección A, serán introducidos en la base de datos de la UE por el proveedor o, en su caso, por el representante autorizado.

2 bis. Los datos enumerados en el anexo VIII, sección B, serán introducidos en la base de datos de la UE por el responsable del despliegue que sea o actúe en nombre de autoridades, agencias u organismos públicos, de conformidad con los apartados 1 bis y 1 ter del artículo 51.

3. Con excepción de la sección contemplada en el artículo 51, apartado 1, letra c), y en el artículo 54 bis, apartado 5, la información contenida en la base de datos de la UE registrada de conformidad con el artículo 51 deberá ser accesible y estar a disposición del público de forma fácil de utilizar. La información deberá ser fácilmente navegable y legible por máquina. La información registrada de conformidad con el artículo 54 bis sólo será accesible a las autoridades de vigilancia del mercado y a la Comisión, a menos que el proveedor o prestador potencial haya dado su consentimiento para que esta información sea también accesible al público.

4. La base de datos de la UE contendrá datos personales únicamente en la medida en que sea necesario para recoger y tratar información de conformidad con el presente Reglamento. Dicha información incluirá los nombres y datos de contacto de las personas físicas responsables del registro del sistema y con autoridad legal para representar al proveedor o al implantador, según proceda.

5. La Comisión será el controlador de la base de datos de la UE. Pondrá a disposición de los proveedores, posibles proveedores e implantadores un apoyo técnico y administrativo adecuado. La base de datos cumplirá los requisitos de accesibilidad aplicables.

TÍTULO VIII

# SEGUIMIENTO POSTCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN, VIGILANCIA DEL MERCADO

## Capítulo 1
## SEGUIMIENTO POSTERIOR A LA COMERCIALIZACIÓN

*Artículo 61*

**Seguimiento postcomercialización por parte de los proveedores y plan de seguimiento postcomercialización para los sistemas de IA de alto riesgo**

1. Los proveedores establecerán y documentarán un sistema de seguimiento postcomercialización de manera proporcionada a la naturaleza de las tecnologías de inteligencia artificial y a los riesgos del sistema de IA de alto riesgo.

2. El sistema de seguimiento poscomercialización recopilará, documentará y analizará de forma activa y sistemática los datos pertinentes que puedan facilitar los implantadores o que puedan recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo a lo largo de su vida útil, y permitirá al proveedor evaluar la conformidad continua de los sistemas de IA con los requisitos establecidos en el título III, capítulo 2. Cuando proceda, el seguimiento posterior a la comercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no cubrirá los datos operativos sensibles de los implantadores que sean autoridades policiales.

3. El sistema de seguimiento poscomercialización se basará en un plan de seguimiento poscomercialización. El plan de seguimiento poscomercialización formará parte de la documentación técnica a que se refiere el Anexo IV. A más tardar seis meses antes de la entrada en vigor del presente Reglamento, la Comisión adoptará un acto de ejecución por el que se establezcan disposiciones detalladas para la plantilla del plan de seguimiento poscomercialización y la lista de elementos que deben incluirse en el plan.

4. En el caso de los sistemas de IA de alto riesgo cubiertos por los actos jurídicos mencionados en la sección A del anexo II, cuando ya se haya establecido un sistema y un plan de seguimiento poscomercialización en virtud de dicha legislación, con el fin de garantizar la coherencia, evitar duplicaciones y minimizar las cargas adicionales, los proveedores tendrán la opción de integrar, según proceda, los elementos necesarios

descritos en los apartados 1, 2 y 3 utilizando la plantilla mencionada en el apartado 3 en un sistema y plan ya existentes con arreglo a la legislación de armonización de la Unión enumerada en la sección A del anexo II, siempre que alcance un nivel de protección equivalente.

El párrafo primero se aplicará también a los sistemas de IA de alto riesgo a que se refiere el punto 5 del anexo III comercializados o puestos en servicio por entidades financieras que estén sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación de la Unión en materia de servicios financieros.

# Capítulo 2

# INTERCAMBIO DE INFORMACIÓN SOBRE INCIDENTES GRAVES

*Artículo 62*

**Notificación de incidentes graves**

1. Los proveedores de sistemas de IA de alto riesgo comercializados en el mercado de la Unión informarán de cualquier incidente grave a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya producido dicho incidente.

1 bis. Por regla general, el plazo para la notificación a que se refiere el apartado 1 tendrá en cuenta la gravedad del incidente grave.

1 ter. La notificación a que se refiere el apartado 1 se efectuará inmediatamente después de que el proveedor haya establecido un nexo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista tal nexo y, en cualquier caso, a más tardar 15 días después de que el proveedor o, en su caso, el implantador, tenga conocimiento del incidente grave.

1 quater. No obstante lo dispuesto en el apartado 1 ter, en caso de infracción generalizada o de incidente grave, tal como se definen en el artículo 3, apartado 44, letra b), el informe a que se refiere el apartado 1 se facilitará inmediatamente, y a más tardar 2 días después de que el proveedor o, en su caso, el implantador tenga conocimiento de dicho incidente.

1 quinquies No obstante lo dispuesto en el apartado 1 ter, en caso de fallecimiento de una persona, el informe se facilitará inmediatamente después de que el proveedor o el encargado de la implantación haya establecido o tan pronto como sospeche que existe una relación causal entre el sistema de IA de alto riesgo y el incidente grave, pero a más tardar diez días después de la fecha en que el proveedor o, en su caso, el encargado de la implantación tenga conocimiento del incidente grave.

1e. Cuando sea necesario para garantizar la puntualidad de los informes, el proveedor o, en su caso, el encargado del despliegue, podrá presentar un informe inicial incompleto seguido de un informe completo.

1 bis.Tras la notificación de un incidente grave con arreglo al párrafo primero, el proveedor realizará sin demora las investigaciones necesarias en relación con el incidente grave y el sistema de IA afectado. Esto incluirá una evaluación del riesgo del incidente y medidas correctoras. El proveedor cooperará con las autoridades competentes y, en su caso, con el organismo notificado afectado durante las investigaciones a que se refiere el párrafo primero y no llevará a cabo ninguna investigación que implique la alteración del sistema de IA afectado de manera que pueda afectar a cualquier evaluación posterior de las causas del incidente, antes de informar a las autoridades competentes de dicha acción.

2. Al recibir una notificación relacionada con un incidente grave contemplado en el artículo 3, apartado 44, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales contemplados en el artículo 64, apartado 3. 2. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1. Dichas orientaciones se publicarán doce meses después de la notificación. Dichas orientaciones se publicarán a más tardar 12 meses después de la entrada en vigor del presente Reglamento y se evaluarán periódicamente.

2 bis. La autoridad de vigilancia del mercado adoptará las medidas adecuadas, según lo dispuesto en el artículo 19 del Reglamento 2019/1020, en un plazo de 7 días a partir de la fecha en que haya recibido la notificación a que se refiere el apartado 1 y seguirá los procedimientos de notificación previstos en el Reglamento 2019/1020.

3. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III que sean comercializados o puestos en servicio por proveedores sujetos a instrumentos legislativos de la Unión que establezcan obligaciones de notificación equivalentes a las establecidas en el presente Reglamento, la notificación de incidentes graves se limitará a los contemplados en el artículo 3, apartado 44, letra c).

3 bis. Para los sistemas de IA de alto riesgo que sean componentes de seguridad de productos, o sean ellos mismos productos, cubiertos por el Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746, la notificación de incidentes graves se limitará a los contemplados en el artículo 3, apartado 44, letra c), y se realizará a la autoridad nacional competente elegida a tal efecto por los Estados miembros en los que se haya producido dicho incidente.

3 bis.Las autoridades nacionales competentes notificarán inmediatamente a la Comisión cualquier incidente grave, haya tomado o no medidas al respecto, de conformidad con el artículo 20 del Reglamento 2019/1020.

# Capítulo 3 APLICACIÓN

*Artículo 63*

**Vigilancia del mercado y control de los sistemas de IA en el mercado de la Unión**

1. El Reglamento (UE) 2019/1020 se aplicará a los sistemas de IA cubiertos por el presente Reglamento. No obstante, a efectos de la aplicación efectiva del presente Reglamento:

(a) cualquier referencia a un operador económico en virtud del Reglamento (UE) 2019/1020 se entenderá que incluye a todos los operadores identificados en el artículo 2, apartado 1, del presente Reglamento;

(b) toda referencia a un producto con arreglo al Reglamento (UE) 2019/1020 se entenderá que incluye todos los sistemas de IA incluidos en el ámbito de aplicación del presente Reglamento.

2. Como parte de sus obligaciones de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado comunicarán anualmente a la Comisión y a las autoridades nacionales de competencia pertinentes cualquier información identificada en el curso de las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación del Derecho de la Unión en materia de normas de competencia. También informarán anualmente a la Comisión sobre el uso de prácticas prohibidas que se haya producido durante ese año y sobre las medidas adoptadas.

3. Para los sistemas de IA de alto riesgo, relacionados con los productos a los que se aplican los actos jurídicos enumerados en la sección A del anexo II, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designada en virtud de dichos actos jurídicos. No obstante lo dispuesto en el párrafo anterior, en circunstancias justificadas, los Estados miembros podrán designar a otra autoridad pertinente para que actúe como autoridad de vigilancia del mercado, siempre que se garantice la coordinación con las autoridades sectoriales pertinentes de vigilancia del mercado responsables de la aplicación de los actos jurídicos enumerados en el anexo II.

3 bis. Los procedimientos contemplados en los artículos 65, 66, 67 y 68 del presente Reglamento no se aplicarán a los sistemas de IA relacionados con productos a los que se apliquen los actos jurídicos enumerados en la sección A del anexo II, cuando dichos actos jurídicos ya prevean procedimientos que garanticen un nivel de protección equivalente y tengan el mismo objetivo. En tal caso, se aplicarán en su lugar dichos procedimientos sectoriales.

3 ter. Sin perjuicio de las competencias de las autoridades de vigilancia del mercado previstas en el artículo 14 del Reglamento 2019/1020, a efectos de garantizar el cumplimiento efectivo de la presente

Reglamento, las autoridades de vigilancia del mercado podrán ejercer las competencias contempladas en el artículo 14, apartado 4, letras d) y j), del Reglamento 2019/1020 a distancia, según proceda.

4. Para los sistemas de IA de alto riesgo comercializados, puestos en servicio o utilizados por entidades financieras reguladas por la legislación de la Unión sobre servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad nacional pertinente responsable de la supervisión financiera de dichas entidades con arreglo a dicha legislación, en la medida en que la comercialización, puesta en servicio o utilización del sistema de IA esté en relación directa con la prestación de dichos servicios financieros.

4 bis. No obstante lo dispuesto en el párrafo anterior, en circunstancias justificadas y siempre que se garantice la coordinación, el Estado miembro podrá designar a otra autoridad pertinente como autoridad de vigilancia del mercado a efectos del presente Reglamento.

Las autoridades nacionales de vigilancia del mercado que supervisen entidades de crédito reguladas con arreglo a la Directiva 2013/36/UE, que participen en el Mecanismo Único de Supervisión (MUS) establecido por el Reglamento n.º 1204/2013 del Consejo, deben comunicar sin demora al Banco Central Europeo toda información detectada en el curso de sus actividades de vigilancia del mercado que pueda ser de interés potencial para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

5. Para los sistemas de IA de alto riesgo enumerados en el punto 1 en la medida en que los sistemas se utilicen con fines policiales y para los fines enumerados en los puntos 6, 7 y 8 del anexo III, los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control competentes en materia de protección de datos en virtud del Reglamento 2016/679, o de la Directiva (UE) 2016/680, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 1 a 44 de la Directiva o de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades cuando actúen en el ejercicio de sus funciones jurisdiccionales.

6. Cuando las instituciones, agencias y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como su autoridad de vigilancia del mercado, salvo en lo que respecta al Tribunal de Justicia en el ejercicio de sus funciones jurisdiccionales.

7. Los Estados miembros facilitarán la coordinación entre las autoridades de vigilancia del mercado designadas en virtud del presente Reglamento y otras autoridades u organismos nacionales pertinentes que supervisen la aplicación de la legislación de armonización de la Unión enumerada en el anexo II o de otra legislación de la Unión que pueda ser pertinente para los sistemas de IA de alto riesgo mencionados en el anexo III.

7 bis. Las autoridades de vigilancia del mercado y la Comisión podrán proponer actividades conjuntas, incluidas investigaciones conjuntas, que llevarán a cabo las autoridades de vigilancia del mercado o las autoridades de vigilancia del mercado conjuntamente con la Comisión, con el objetivo de promover el cumplimiento, identificar el incumplimiento, aumentar la sensibilización y proporcionar orientación en relación con el presente Reglamento con respecto a categorías específicas de sistemas de IA de alto riesgo que se considere que presentan un riesgo grave en varios Estados miembros de conformidad con el artículo 9 del Reglamento 2019/1020. La Oficina de Inteligencia Artificial prestará apoyo a la coordinación de las investigaciones conjuntas.

7 bis. Sin perjuicio de las competencias previstas en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, el proveedor concederá a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de formación, validación y ensayo utilizados para el desarrollo del sistema de IA de alto riesgo, incluso, cuando proceda y con sujeción a las salvaguardias de seguridad, a través de interfaces de programación de aplicaciones ("API") u otros medios técnicos y herramientas pertinentes que permitan el acceso a distancia.

7 ter. Se concederá a las autoridades de vigilancia del mercado acceso al código fuente del sistema de IA de alto riesgo previa solicitud motivada y sólo cuando se cumplan las siguientes condiciones acumulativas:

(a) el acceso al código fuente es necesario para evaluar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del título III; y

(b) se han agotado o han resultado insuficientes los procedimientos de comprobación/auditoría y las verificaciones basadas en los datos y la documentación facilitados por el proveedor.

7c. Toda información y documentación obtenida por las autoridades de vigilancia del mercado se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 70.

*Artículo 63 bis*

**Asistencia mutua, vigilancia del mercado y control de los sistemas de IA de propósito general**

1. Cuando un sistema de IA se base en un modelo de IA de propósito general y el modelo y el sistema sean desarrollados por el mismo proveedor, la Oficina de IA tendrá competencias para vigilar y supervisar el cumplimiento de las obligaciones del presente Reglamento por parte de este sistema de IA. Para llevar a cabo las tareas de seguimiento y supervisión, la Oficina de IA tendrá todas las competencias de una autoridad de vigilancia del mercado en el sentido del Reglamento 2019/1020.

Cuando las autoridades de vigilancia del mercado pertinentes tengan motivos suficientes para considerar que los sistemas de IA de propósito general que puedan ser utilizados directamente por los implantadores para al menos un fin clasificado como de alto riesgo con arreglo al presente Reglamento, incumplen los requisitos establecidos en el presente Reglamento, cooperarán con la Oficina de IA para llevar a cabo la evaluación del cumplimiento e informarán de ello al Consejo y a las demás autoridades de vigilancia del mercado.

2. Cuando una autoridad nacional de vigilancia del mercado no pueda concluir su investigación sobre el sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA de propósito general a pesar de haber realizado todos los esfuerzos adecuados para obtener dicha información, podrá presentar una solicitud motivada a la Oficina de IA en la que se pueda exigir el acceso a esta información. En este caso, la Oficina de IA facilitará a la autoridad solicitante sin demora, y en cualquier caso en un plazo de 30 días, cualquier información que la Oficina de IA considere pertinente para determinar si un sistema de IA de alto riesgo no es conforme. Las autoridades nacionales del mercado salvaguardarán la confidencialidad de la información que obtengan de conformidad con el artículo 70. Se aplicará por analogía el procedimiento previsto en el capítulo VI del Reglamento (UE) 1020/2019.

*Artículo 63 ter*

**Supervisión de las pruebas en condiciones reales por parte de las autoridades de vigilancia del mercado**

1. Las autoridades de vigilancia del mercado tendrán la competencia y las facultades necesarias para garantizar que los ensayos en condiciones reales sean conformes al presente Reglamento.

2. Cuando se realicen ensayos en condiciones reales para sistemas de IA supervisados dentro de un espacio aislado regulador de la IA con arreglo al artículo 54, las autoridades de vigilancia del mercado verificarán el cumplimiento de las disposiciones del artículo 54 bis como parte de su función de supervisión del espacio aislado regulador de la IA. Dichas autoridades podrán, en su caso, permitir que el proveedor o posible proveedor realice las pruebas en condiciones reales como excepción a las condiciones establecidas en el artículo 54 bis, apartado 4, letras f) y g).

3. Cuando una autoridad de vigilancia del mercado haya sido informada por el proveedor potencial, el proveedor o cualquier tercero de un incidente grave o tenga otros motivos para considerar que no se cumplen las condiciones establecidas en los artículos 54 bis y 54 ter, podrá adoptar en su territorio cualquiera de las siguientes decisiones, según proceda:

(a) suspender o finalizar las pruebas en condiciones reales;

exigir al proveedor o posible proveedor y al usuario o usuarios que modifiquen cualquier aspecto de las pruebas en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión de las contempladas en el apartado 3 del presente artículo o haya formulado una objeción en el sentido del artículo 54 bis, apartado 4, letra b), la decisión o la objeción indicarán los motivos de la misma y las modalidades y condiciones para que el proveedor o posible proveedor impugne la decisión o la objeción.

5. En su caso, cuando una autoridad de vigilancia del mercado haya adoptado una decisión de las contempladas en el apartado 3 del presente artículo, comunicará los motivos de la misma a las autoridades de vigilancia del mercado de los demás Estados miembros en los que se haya sometido a ensayo el sistema de IA de conformidad con el plan de ensayo.

*Artículo 64*

**Competencias de las autoridades de protección de los derechos fundamentales**

3. Las autoridades u organismos públicos nacionales que supervisen o hagan cumplir las obligaciones derivadas del Derecho de la Unión que protegen los derechos fundamentales, incluido el derecho a la no discriminación, en relación con el uso de los sistemas de IA de alto riesgo a que se refiere el anexo III estarán facultados para solicitar y acceder a cualquier documentación creada o conservada en virtud del presente Reglamento en una lengua y formato accesibles cuando el acceso a dicha documentación sea necesario para el cumplimiento efectivo de su mandato dentro de los límites de su jurisdicción. La autoridad u organismo público pertinente informará de dicha solicitud a la autoridad de vigilancia del mercado del Estado miembro de que se trate.

4. A más tardar tres meses después de la entrada en vigor del presente Reglamento, cada Estado miembro identificará a las autoridades u organismos públicos a que se refiere el apartado 3 y pondrá una lista a disposición del público. Los Estados miembros notificarán la lista a la Comisión y a todos los demás Estados miembros y la mantendrán actualizada.

5. Cuando la documentación a que se refiere el apartado 3 sea insuficiente para determinar si se ha producido un incumplimiento de las obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 3 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para que organice la comprobación del sistema de IA de alto riesgo por medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la estrecha participación de la autoridad u organismo público solicitante en un plazo razonable a partir de la solicitud.

Toda información y documentación obtenida por las autoridades u organismos públicos nacionales a que se refiere el apartado 3 en virtud de lo dispuesto en el presente artículo se tratará respetando las obligaciones de confidencialidad establecidas en el artículo 70.

*Artículo 65*

**Procedimiento para tratar los sistemas de IA que presentan un riesgo a nivel nacional**

1. Se entenderá por sistemas de IA que presentan un riesgo un producto que presenta un riesgo definido en el artículo 3, punto 19, del Reglamento (UE) 2019/1020 en lo que respecta a los riesgos para la salud o la seguridad o para los derechos fundamentales de las personas.

2. Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo de los contemplados en el apartado 1, llevará a cabo una evaluación del sistema de IA en cuestión con respecto a su conformidad con todos los requisitos y obligaciones establecidos en el presente Reglamento. Se prestará especial atención a los sistemas de IA que presenten un riesgo para los grupos vulnerables (contemplados en el artículo 5). Cuando se detecten riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 64, apartado 3, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en la medida de lo necesario con la autoridad de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 64, apartado 3.

Cuando, en el transcurso de esa evaluación, la autoridad de vigilancia del mercado y, en su caso, en cooperación con la autoridad pública nacional a que se refiere el artículo 64, apartado 3, compruebe que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al agente económico pertinente que adopte todas las medidas correctoras adecuadas para que el sistema de IA sea conforme, retirarlo del mercado o recuperarlo en el plazo que ella prescriba y, en cualquier caso, a más tardar en quince días hábiles o en el plazo que establezca la legislación de armonización de la Unión pertinente, según proceda.

La autoridad de vigilancia del mercado informará de ello al organismo notificado pertinente. El artículo 18 del Reglamento (UE) 2019/1020 se aplicará a las medidas contempladas en el párrafo segundo.

3. Cuando la autoridad de vigilancia del mercado considere que el incumplimiento no se limita a su territorio nacional, informará a la Comisión, y a los demás Estados miembros sin

demora indebida de los resultados de la evaluación y de las medidas que ha exigido que adopte el operador.

4. El operador velará por que se adopten todas las medidas correctoras oportunas en relación con todos los sistemas de IA afectados que haya comercializado en toda la Unión.

5. 3. Si el operador de un sistema de IA no adopta las medidas correctoras adecuadas en el plazo indicado en el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales apropiadas para prohibir o restringir la comercialización o puesta en servicio del sistema de IA en su mercado nacional, retirar el producto o el sistema de IA autónomo de dicho mercado o recuperarlo. Dicha autoridad notificará sin demora indebida dichas medidas a la Comisión y a los demás Estados miembros.

6. La notificación a que se refiere el apartado 5 incluirá todos los detalles disponibles, en particular la información necesaria para la identificación del sistema de IA no conforme, el origen del sistema de IA y la cadena de suministro, la naturaleza del supuesto incumplimiento y el riesgo que entraña, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos esgrimidos por el agente económico pertinente. En particular, las autoridades de vigilancia del mercado indicarán si el incumplimiento se debe a uno o varios de los siguientes factores:

(-a) incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5;

(a) el incumplimiento por parte de un sistema de IA de alto riesgo de los requisitos establecidos en el Capítulo 2 del Título III;

(b) las deficiencias de las normas armonizadas o especificaciones comunes contempladas en los artículos 40 y 41 que confieren una presunción de conformidad;

(b bis) incumplimiento de las disposiciones establecidas en el artículo 52.

7. Las autoridades de vigilancia del mercado de los Estados miembros distintas de la autoridad de vigilancia del mercado del Estado miembro que haya iniciado el procedimiento informarán sin demora indebida a la Comisión y a los demás Estados miembros de toda medida que adopten y de cualquier dato adicional sobre la no conformidad del sistema de IA de que dispongan y, en caso de desacuerdo con la medida nacional notificada, presentarán sus objeciones al respecto.

8. Cuando, en el plazo de tres meses a partir de la recepción de la notificación a que se refiere el apartado 5, ni una autoridad de vigilancia del mercado de un Estado miembro ni la Comisión hayan formulado objeciones con respecto a una medida provisional adoptada por una autoridad de vigilancia del mercado de otro Estado miembro, dicha medida se considerará justificada. Ello sin

perjuicio de los derechos procesales del operador afectado de conformidad con el artículo 18 del Reglamento (UE) 2019/1020. El plazo a que se refiere la primera frase del presente apartado se reducirá a treinta días en caso de incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5.

9. Las autoridades de vigilancia del mercado de todos los Estados miembros velarán por que se adopten las medidas restrictivas adecuadas con respecto al producto o al sistema de IA en cuestión, como la retirada del producto o del sistema de IA de su mercado, sin demoras indebidas.

*Artículo 65 bis*

**Procedimiento para tratar los sistemas de IA clasificados por el proveedor como de riesgo no elevado en aplicación del anexo III**

1. Cuando una autoridad de vigilancia del mercado tenga motivos suficientes para considerar que un sistema de IA clasificado por el proveedor como de riesgo no alto en aplicación del anexo III es de alto riesgo, llevará a cabo una evaluación del sistema de IA en cuestión con respecto a su clasificación como sistema de IA de alto riesgo basándose en las condiciones establecidas en el anexo III y en las directrices de la Comisión.

2. Cuando, en el transcurso de dicha evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA en cuestión es de alto riesgo, exigirá sin demora indebida al proveedor pertinente que tome todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento, así como que adopte las medidas correctoras adecuadas en un plazo que podrá fijar.

3. Cuando la autoridad de vigilancia del mercado considere que el uso del sistema de IA en cuestión no se limita a su territorio nacional, informará sin demora indebida a la Comisión y a los demás Estados miembros de los resultados de la evaluación y de las medidas que haya exigido que adopte el proveedor.

4. El proveedor velará por que se adopten todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento. 3. Cuando el proveedor de un sistema de IA de que se trate no haga que el sistema de IA cumpla los requisitos y obligaciones del presente Reglamento en el plazo mencionado en el apartado 2, se le impondrán multas de conformidad con el artículo 71.

5. El proveedor velará por que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en toda la Unión.

Si el proveedor del sistema de IA en cuestión no adopta las medidas correctoras adecuadas en el plazo mencionado en el apartado 2, se aplicarán las disposiciones de los apartados 5 a 9 del artículo 65.

6. Cuando, en el transcurso de dicha evaluación con arreglo al apartado 1, la autoridad de vigilancia del mercado establezca que el sistema de IA fue clasificado erróneamente por el proveedor como de no alto riesgo para eludir la aplicación de los requisitos del capítulo 2 del título III, el proveedor estará sujeto a multas de conformidad con el artículo 71.

7. En el ejercicio de su facultad de controlar la aplicación del presente artículo y de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado podrán realizar las comprobaciones oportunas, teniendo en cuenta, en particular, la información almacenada en la base de datos de la UE a que se refiere el artículo 60.

*Artículo 66*

**Procedimiento de salvaguardia de la Unión**

1. Cuando, en el plazo de tres meses a partir de la recepción de la notificación a que se refiere el artículo 65, apartado 5, o de 30 días en caso de incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5, la autoridad de vigilancia del mercado de un Estado miembro formule objeciones contra una medida adoptada por otra autoridad de vigilancia del mercado, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión consultará sin demora indebida a la autoridad de vigilancia del mercado del Estado miembro y al operador u operadores pertinentes y evaluará la medida nacional. Sobre la base de los resultados de dicha evaluación, la Comisión decidirá si la medida nacional está o no justificada en un plazo de seis meses, o de 60 días en caso de incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5, a partir de la notificación a que se refiere el artículo 65, apartado 5, y notificará dicha decisión a la autoridad de vigilancia del mercado del Estado miembro de que se trate. La Comisión informará asimismo de dicha decisión a todas las demás autoridades de vigilancia del mercado.

2. Si la Comisión considera que la medida adoptada por los Estados miembros pertinentes está justificada, todos los Estados miembros velarán por que se adopten las medidas restrictivas adecuadas con respecto al sistema de IA en cuestión, como la retirada del sistema de IA de su mercado sin demora injustificada, e informarán de ello a la Comisión. Si la Comisión considera injustificada la medida nacional, el Estado miembro afectado retirará la medida e informará a la Comisión en consecuencia.

Cuando la medida nacional se considere justificada y la no conformidad del sistema de IA se atribuya a deficiencias de las normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41 del presente Reglamento, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) nº 1025/2012.

*Artículo 67*

**Sistemas de IA que presentan un riesgo**

1. Cuando, habiendo realizado una evaluación con arreglo al artículo 65, previa consulta a la autoridad pública nacional pertinente a que se refiere el artículo 64, apartado 3, la autoridad de vigilancia del mercado de un Estado miembro compruebe que, aunque un sistema de IA de alto riesgo es conforme con el presente Reglamento, presenta un riesgo para la salud o la seguridad de las personas, los derechos fundamentales u otros aspectos de la protección del interés público, exigirá al operador pertinente que adopte todas las medidas adecuadas para garantizar que el sistema de IA en cuestión, cuando se comercialice o se ponga en servicio, deje de presentar ese riesgo sin demora indebida, en un plazo que podrá fijar.

2. El proveedor u otros operadores pertinentes velarán por que se adopten medidas correctoras en relación con todos los sistemas de IA afectados que hayan comercializado en toda la Unión dentro del plazo establecido por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. Los Estados miembros informarán inmediatamente a la Comisión y a los demás Estados miembros. Dicha información incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación del sistema de IA de que se trate, el origen y la cadena de suministro del sistema de IA, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión consultará sin demora indebida a los Estados miembros afectados y al operador pertinente y evaluará las medidas nacionales adoptadas. Sobre la base de los resultados de dicha evaluación, la Comisión decidirá si la medida está justificada o no y, en su caso, propondrá las medidas adecuadas.

5. La Comisión comunicará inmediatamente su decisión a los Estados miembros afectados y a los operadores pertinentes. También informará de la decisión a todos los demás Estados miembros.

*Artículo 68*

**Incumplimiento formal**

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro llegue a una de las siguientes conclusiones, exigirá al proveedor en cuestión que ponga fin al incumplimiento de que se trate, en un plazo que podrá fijar:

(a) se ha colocado el marcado CE infringiendo el artículo 49;

(b) no se ha colocado el marcado CE;

(c) no se ha elaborado la declaración de conformidad de la UE;

(d) la declaración UE de conformidad no se ha redactado correctamente; e bis) no se ha efectuado el registro en la base de datos de la UE;

(e ter) en su caso, no se ha designado al representante autorizado; ec) no se dispone de la documentación técnica.

2. Si persiste el incumplimiento a que se refiere el apartado 1, la autoridad de vigilancia del mercado del Estado miembro en cuestión adoptará las medidas adecuadas y proporcionadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o garantizar su recuperación o retirada del mercado sin demora.

*Artículo 68 bis*

**Estructuras de apoyo a las pruebas de IA de la UE en el ámbito de la inteligencia artificial**

1. La Comisión designará una o varias estructuras de apoyo a las pruebas de IA de la UE para realizar las tareas enumeradas en el artículo 21, apartado 6, del Reglamento (UE) 1020/2019 en el ámbito de la inteligencia artificial.

2. Sin perjuicio de las tareas mencionadas en el apartado 1, la estructura de apoyo a las pruebas de IA de la UE también proporcionará asesoramiento técnico o científico independiente a petición del Consejo, la Comisión o las autoridades de vigilancia del mercado.

# Capítulo 3b REMEDIOS

*Artículo 68 bis*

**Derecho a presentar una reclamación ante una autoridad de vigilancia del mercado**

1. Sin perjuicio de otros recursos administrativos o judiciales, cualquier persona física o jurídica que tenga motivos para considerar que se ha producido una infracción de las disposiciones del presente Reglamento podrá presentar una reclamación ante la autoridad de vigilancia del mercado competente.

2. De conformidad con el Reglamento (UE) 2019/1020, las reclamaciones se tendrán en cuenta a efectos de la realización de las actividades de vigilancia del mercado y se tramitarán en consonancia con los procedimientos específicos establecidos al efecto por las autoridades de vigilancia del mercado

*Artículo 68 quater*

**Derecho a una explicación de la toma de decisiones individual**

1. Toda persona afectada que sea objeto de una decisión adoptada por el responsable del despliegue sobre la base de los resultados de un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas enumerados en el punto 2, y que produzca efectos jurídicos o le afecte significativamente de manera similar de forma que considere que repercute negativamente en su salud, seguridad y derechos fundamentales, tendrá derecho a solicitar al responsable del despliegue explicaciones claras y significativas sobre el papel del sistema de IA en el procedimiento de toma de decisiones y los principales elementos de la decisión adoptada.

2. El apartado 1 no se aplicará al uso de sistemas de IA para los que se deriven excepciones o restricciones a la obligación establecida en el apartado 1 del Derecho de la Unión o nacional en cumplimiento del Derecho de la Unión.

3. El presente artículo sólo se aplicará en la medida en que el derecho contemplado en el apartado 1 no esté ya previsto en la legislación de la Unión.

*Artículo 68 quinquies*

**Modificación de la Directiva (UE) 2020/1828**

En el anexo I de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo[30] , se añade el siguiente punto: "(67 bis) Reglamento xxxx/xxxx del Parlamento Europeo y del Consejo [por el que se establecen normas armonizadas sobre inteligencia artificial (Ley sobre inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L ...)]".

*Artículo 68 sexies*

**Notificación de infracciones y protección de los denunciantes**

La Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo se aplicará a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien dichas infracciones.

# Capítulo 3c

# SUPERVISIÓN, INVESTIGACIÓN, APLICACIÓN Y CONTROL DE LOS PROVEEDORES DE MODELOS AI DE USO GENERAL

*Artículo 68 septies*

**Cumplimiento de las obligaciones de los proveedores de modelos de IA de propósito general**

1. La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el capítulo/título [modelos de IA de propósito general] teniendo en cuenta las garantías procesales en virtud del artículo 68 quaterdecies. La Comisión confiará la ejecución de estas tareas a la Oficina Europea de IA, sin perjuicio de las competencias de organización de la Comisión.

---

**30** Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

y el reparto de competencias entre los Estados miembros y la Unión basado en los Tratados.

2. Sin perjuicio de lo dispuesto en el apartado 3 del artículo 63 bis, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las competencias establecidas en el presente capítulo, cuando ello sea necesario y proporcionado para ayudarles en el cumplimiento de sus funciones con arreglo al presente Reglamento.

*Artículo 68 octies*

**Acciones de seguimiento**

1. Para llevar a cabo las tareas que le asigna el presente capítulo, la Oficina de IA podrá adoptar las medidas necesarias para supervisar la aplicación efectiva y el cumplimiento del presente Reglamento por parte de los proveedores de modelos de IA de uso general, incluida la adhesión a los códigos de prácticas aprobados.

2. Los proveedores intermedios tendrán derecho a presentar una denuncia por presunta infracción del presente Reglamento. Las reclamaciones deberán estar debidamente motivadas y, como mínimo, indicar:

(a) el punto de contacto del proveedor del modelo de IA de propósito general de que se trate;

(b) descripción de los hechos pertinentes, las disposiciones del presente Reglamento afectadas y la razón por la que el proveedor de servicios posteriores considera que el proveedor del modelo de IA de propósito general en cuestión ha infringido el presente Reglamento;

(c) cualquier otra información que el proveedor intermedio que envió la solicitud considere pertinente, incluida, en su caso, la información recabada por iniciativa propia.

*Artículo 68 nonies*

**Alertas de riesgos sistémicos por el panel científico**

1. La comisión técnica científica podrá enviar una alerta cualificada a la Oficina de AI cuando tenga motivos para sospechar que

(a) un modelo de IA de propósito general plantea un riesgo concreto identificable a nivel de la Unión; o

(b) un modelo de IA de propósito general cumple los requisitos contemplados en el artículo 52 bis [*Clasificación de los modelos de IA de propósito general con riesgo sistémico*].

2. A partir de dicha descripción cualificada, la Comisión, a través de la Oficina AI y tras haber informado al Consejo AI, podrá ejercer las competencias previstas en el presente Capítulo a efectos

de evaluar el asunto. La Oficina de AI informará al Consejo de cualquier medida adoptada con arreglo a los artículos 68 decies a 68 quaterdecies.

3. Una descripción cualificada deberá estar debidamente motivada y al menos indicar:

(a) el punto de contacto del proveedor del modelo de IA de propósito general con el riesgo sistémico en cuestión;

(b) una descripción de los hechos relevantes y las razones de la sospecha del panel científico;

(c) cualquier otra información que la comisión técnica científica considere pertinente, incluida, en su caso, la información recabada por iniciativa propia.

*Artículo 68 decies*

**Facultad de solicitar documentación e información**

1. La Comisión podrá solicitar al proveedor del modelo de IA de propósito general de que se trate que facilite la documentación elaborada por el proveedor con arreglo a los artículos 52 quater [Obligaciones de los proveedores de modelos de IA de propósito general] y 52 quinquies [Obligaciones de los proveedores de modelos de IA de propósito general con riesgo sistémico] o cualquier información adicional que resulte necesaria para evaluar el cumplimiento del presente Reglamento por parte del proveedor.

2. Antes de enviar la solicitud de información, la Oficina de IA podrá iniciar un diálogo estructurado con el proveedor del modelo de IA de propósito general.

3. Previa solicitud debidamente justificada de la comisión técnica científica, la Comisión podrá emitir una solicitud de información a un proveedor de un modelo de IA de propósito general, cuando el acceso a la información sea necesario y proporcionado para el cumplimiento de las tareas de la comisión técnica científica con arreglo al artículo 58 ter [*Comisión técnica científica*](2).

4. En la solicitud de información se hará constar la base jurídica y el objeto de la solicitud, especificando qué información se requiere y fijando el plazo en el que deberá facilitarse la información, así como las multas previstas en el artículo 72 bis [*multas*] por facilitar información incorrecta, incompleta o engañosa.

5. El proveedor del modelo de IA de propósito general de que se trate o sus representantes y, en el caso de personas jurídicas, sociedades o empresas, o cuando carezcan de personalidad jurídica, las personas autorizadas a representarlas por ley o por sus estatutos, suministrarán la información solicitada en nombre del proveedor del modelo de IA de propósito general de que se trate. Los abogados debidamente autorizados para actuar podrán facilitar la información en nombre de sus clientes. Estos últimos serán plenamente responsables si la información facilitada es incompleta,

incorrecta o engañosa.

*Artículo 68 undecies*

**Poder para realizar evaluaciones**

1. La Oficina de IA, previa consulta al Consejo, podrá realizar evaluaciones del modelo de IA de propósito general de que se trate

(a) evaluar el cumplimiento por parte del prestador de las obligaciones derivadas del presente Reglamento, cuando la información recabada con arreglo al artículo 68 decies [Facultad de solicitar información] sea insuficiente; o bien

(b) investigar los riesgos sistémicos a nivel de la Unión de los modelos de IA *de propósito general con riesgo* sistémico, en particular a raíz de un informe cualificado del panel científico de conformidad con el artículo 68 septies, letra c) [*Cumplimiento de las obligaciones de los proveedores de modelos de IA de propósito general y de modelos de IA de propósito general con riesgo sistémico*](3).

2. La Comisión podrá decidir el nombramiento de expertos independientes para que realicen evaluaciones en su nombre, incluso a partir del panel científico con arreglo al artículo [panel científico de expertos independientes]. Todos los expertos independientes designados para esta tarea deberán cumplir los criterios establecidos en el apartado 2 del artículo 58 ter.

3. A efectos del apartado 1, la Comisión podrá solicitar el acceso al modelo de IA de propósito general de que se trate a través de interfaces de programación de aplicaciones ("API") u otros medios y herramientas técnicos adecuados, incluido el código fuente.

4. En la solicitud de acceso se indicará la base jurídica, el objeto y los motivos de la solicitud y se fijará el plazo en el que debe facilitarse el acceso, así como las multas previstas en el artículo 72 bis [*multas*] por no facilitar el acceso.

5. Los proveedores del modelo de IA de propósito general de que se trate y, en el caso de personas jurídicas, sociedades o empresas, o cuando carezcan de personalidad jurídica, las personas autorizadas a representarlas por ley o por sus estatutos, facilitarán el acceso solicitado en nombre del proveedor del modelo de IA de propósito general de que se trate.

6. Las modalidades y condiciones de las evaluaciones, incluidas las modalidades de participación de expertos independientes y el procedimiento de selección de estos últimos, se establecerán en

actos de ejecución. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 74, apartado 2.

7. Antes de solicitar acceso al modelo de IA de propósito general en cuestión, la Oficina de IA podrá iniciar un diálogo estructurado con el proveedor del modelo de IA de propósito general para recabar más información sobre las pruebas internas del modelo, las salvaguardias internas para prevenir riesgos sistémicos y otros procedimientos y medidas internas que el proveedor haya adoptado para mitigar dichos riesgos.

*Artículo 68 duodecies*

**Poder para solicitar medidas**

1. Cuando sea necesario y oportuno, la Comisión podrá solicitar a los proveedores que

(a) adoptar las medidas adecuadas para cumplir las obligaciones establecidas en el Título VIII bis, Capítulo 2 [Obligaciones del proveedor de modelos de IA de propósito general];

(b) exigir a un proveedor que aplique medidas paliativas, cuando la evaluación realizada de conformidad con el artículo 68 undecies [*Facultad de realizar evaluaciones] haya suscitado una* preocupación grave y justificada de riesgo sistémico a escala de la Unión;

(c) restringir la comercialización, retirar o recuperar el modelo.

2. Antes de solicitar una medida, la Oficina de IA podrá iniciar un diálogo estructurado con el proveedor del modelo de IA de propósito general.

3. Si, durante el diálogo estructurado previsto en el apartado 2, el proveedor del modelo de IA de propósito general con riesgo sistémico ofrece compromisos de aplicar medidas de mitigación para hacer frente a un riesgo sistémico a escala de la Unión, la Comisión podrá, mediante decisión, hacer que estos compromisos sean vinculantes y declarar que no hay más motivos para actuar.

*Artículo 68 quaterdecies*

**Derechos procesales de los operadores económicos del modelo de IA de propósito general**

El artículo 18 del Reglamento (UE) 2019/1020 se aplicará por analogía a los proveedores del modelo de IA de propósito general, sin perjuicio de los derechos procesales más específicos previstos en el presente Reglamento.

TÍTULO IX CÓDIGOS DE CONDUCTA

*Artículo 69*

**Códigos de conducta para la aplicación voluntaria de requisitos específicos**

1. La Oficina de la IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, incluidos los mecanismos de gobernanza conexos, destinados a fomentar la aplicación voluntaria a los sistemas de IA distintos de los sistemas de IA de alto riesgo de algunos o todos los requisitos establecidos en el título III, capítulo 2, del presente Reglamento, teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos.

2. La Oficina de AI y los Estados miembros facilitarán la elaboración de códigos de conducta relativos a la aplicación voluntaria, incluso por parte de los implantadores, de requisitos específicos a todos los sistemas de AI, sobre la base de objetivos claros e indicadores clave de rendimiento para medir la consecución de dichos objetivos, incluidos elementos como, entre otros

(a) elementos aplicables previstos en las directrices éticas europeas para una IA digna de confianza;

(b) evaluar y minimizar el impacto de los sistemas de IA en la sostenibilidad medioambiental, también en lo que respecta a la programación eficiente desde el punto de vista energético, y

técnicas para diseñar, entrenar y utilizar eficazmente la IA;

(c) fomentar la alfabetización en IA, en particular de las personas que se ocupan del desarrollo, el funcionamiento y el uso de la IA;

(d) facilitar un diseño inclusivo y diverso de los sistemas de IA, entre otras cosas mediante la creación de equipos de desarrollo inclusivos y diversos y el fomento de la participación de las partes interesadas en ese proceso;

(e) evaluar y prevenir el impacto negativo de los sistemas de IA sobre las personas o grupos de personas vulnerables, también en lo que respecta a la accesibilidad para las personas con discapacidad, así como sobre la igualdad de género.

3. Los códigos de conducta pueden ser elaborados por proveedores o implantadores individuales de sistemas de IA, por organizaciones que los representen o por ambos, incluso con la participación de

los implantadores y cualquier parte interesada y sus organizaciones representativas, incluidas las organizaciones de la sociedad civil y el mundo académico. Los códigos de conducta pueden abarcar uno o varios sistemas de IA, teniendo en cuenta la similitud de la finalidad prevista de los sistemas pertinentes.

4. La Oficina de AI y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de las PYME, incluidas las de nueva creación, a la hora de fomentar y facilitar la elaboración de códigos de conducta.

# TÍTULO X CONFIDENCIALIDAD Y SANCIONES

*Artículo 70*

**Confidencialidad**

1. La Comisión, las autoridades de vigilancia del mercado y los organismos notificados, así como cualquier otra persona física o jurídica implicada en la aplicación del presente Reglamento, respetarán, de conformidad con el Derecho de la Unión o nacional, la confidencialidad de la información y los datos obtenidos en el desempeño de sus funciones y actividades, de manera que se proteja, en particular:

(a) derechos de propiedad intelectual, así como la información comercial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo que sean de aplicación los supuestos contemplados en el artículo 5 de la Directiva 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas;

(b) la aplicación efectiva del presente Reglamento, en particular a efectos de inspecciones, investigaciones o auditorías;

(ba) intereses públicos y de seguridad nacional;

(c) integridad de los procedimientos penales o administrativos;

(d bis) la integridad de la información clasificada de conformidad con el Derecho de la Unión o nacional.

1 bis. Las autoridades que participen en la aplicación del presente Reglamento con arreglo al apartado 1 solo solicitarán los datos estrictamente necesarios para la evaluación del riesgo que plantea el sistema de IA y para el ejercicio de sus competencias en cumplimiento del presente Reglamento y del Reglamento 2019/1020. Establecerán medidas de ciberseguridad adecuadas y eficaces para proteger la seguridad y confidencialidad de la información y los datos obtenidos.

y suprimirá los datos recogidos en cuanto dejen de ser necesarios para la finalidad para la que fueron solicitados, de conformidad con la legislación nacional o europea aplicable.

2. Sin perjuicio de lo dispuesto en los apartados 1 y 1 bis, la información intercambiada con carácter confidencial entre las autoridades nacionales competentes y entre las autoridades nacionales competentes y la Comisión no se revelará sin consulta previa a la autoridad nacional competente de origen y al responsable del despliegue cuando los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III sean utilizados por las autoridades policiales, de control fronterizo, de inmigración o de asilo, cuando dicha revelación pudiera poner en peligro los intereses de la seguridad pública y nacional. Este intercambio de información no abarcará los datos operativos sensibles en relación con las actividades de las autoridades policiales, de control fronterizo, de inmigración o de asilo.

Cuando las autoridades policiales, de inmigración o de asilo sean los proveedores de los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III, la documentación técnica a que se refiere el anexo IV permanecerá en los locales de dichas autoridades. Dichas autoridades velarán por que las autoridades de vigilancia del mercado a que se refiere el artículo 63, apartados 5 y 6, según proceda, puedan, previa solicitud, acceder inmediatamente a la documentación u obtener una copia de la misma. Únicamente el personal de la autoridad de vigilancia del mercado que posea el nivel adecuado de habilitación de seguridad podrá acceder a dicha documentación o a cualquier copia de la misma.

3. Los apartados 1, [1 bis] y 2 no afectarán a los derechos y obligaciones de la Comisión, de los Estados miembros y de sus autoridades competentes, así como de los organismos notificados, por lo que respecta al intercambio de información y a la difusión de alertas, incluso en el contexto de la cooperación transfronteriza, ni a las obligaciones de las partes interesadas de facilitar información con arreglo al Derecho penal de los Estados miembros.

4. La Comisión y los Estados miembros podrán intercambiar, en caso necesario y de conformidad con las disposiciones pertinentes de los acuerdos internacionales y comerciales, información confidencial con las autoridades reguladoras de terceros países con las que hayan celebrado acuerdos bilaterales o multilaterales de confidencialidad que garanticen un nivel adecuado de confidencialidad.

*Artículo 71*

**Sanciones**

1. En cumplimiento de las condiciones establecidas en el presente Reglamento, los Estados miembros establecerán el régimen de sanciones y otras medidas coercitivas, que podrán incluir también advertencias y medidas no pecuniarias, aplicables a las infracciones del presente Reglamento por parte de los operadores, y adoptarán todas las medidas necesarias para garantizar que sean

correcta y eficazmente y teniendo en cuenta las directrices emitidas por la Comisión en virtud del artículo 82 ter. Las sanciones previstas deberán ser efectivas, proporcionadas y disuasorias. Tendrán en cuenta los intereses de las PYME, incluidas las de nueva creación, y su viabilidad económica.

2. Los Estados miembros notificarán sin demora a la Comisión y a más tardar en la fecha de entrada en vigor de dichas normas y de dichas medidas respectivas, así como cualquier modificación posterior que les afecte.

3. El incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5 se sancionará con multas administrativas de hasta 35 000 000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios total anual a escala mundial correspondiente al ejercicio anterior, si esta cifra es superior.

4. El incumplimiento por parte de un sistema de IA de cualquiera de las siguientes disposiciones relativas a los operadores u organismos notificados, distintas de las establecidas en los artículos 5, se sancionará con multas administrativas de hasta 15 000 000 EUR o, si el infractor es una empresa, de hasta el 3% de su volumen de negocios total anual a escala mundial correspondiente al ejercicio anterior, si esta cifra es superior:

(b) obligaciones de los prestadores con arreglo al artículo 16;

(d) obligaciones de los representantes autorizados en virtud del artículo 25;

(e) obligaciones de los importadores con arreglo al artículo 26;

(f) obligaciones de los distribuidores con arreglo al artículo 27;

(g) obligaciones de los responsables del despliegue con arreglo al artículo 29, apartados 1 a 6 bis;

(h) requisitos y obligaciones de los organismos notificados con arreglo al artículo 33, al artículo 34, apartados 1, 3 y 4, y al artículo 34 bis;

(i) obligaciones de transparencia para proveedores y usuarios con arreglo al artículo 52.

5. El suministro de información incorrecta, incompleta o engañosa a los organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud estará sujeto a multas administrativas de hasta 7 500 000 EUR o, si el infractor es una empresa, de hasta el 1 % de su volumen de negocios total anual a escala mundial correspondiente al ejercicio financiero anterior, si esta cifra es superior.

5 bis. En el caso de las PYME, incluidas las de nueva creación, cada multa a que se refiere el presente artículo ascenderá hasta los porcentajes o el importe a que se refieren los apartados 3, 4 y 5, el que sea inferior de los dos.

6. A la hora de decidir sobre la imposición de una multa administrativa y sobre la cuantía de la misma en cada caso concreto, se tendrán en cuenta todas las circunstancias relevantes del caso específico.

Se tendrá en cuenta la situación y, en su caso, se tendrá en cuenta lo siguiente:

(a) la naturaleza, gravedad y duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA, así como, en su caso, el número de personas afectadas y el nivel de perjuicio sufrido por éstas;

(b) si otras autoridades de vigilancia del mercado de uno o más Estados miembros ya han aplicado multas administrativas al mismo operador por la misma infracción;

(b bis) si otras autoridades ya han aplicado multas administrativas al mismo operador por infracciones de otro Derecho de la Unión o nacional, cuando tales infracciones se deriven de la misma actividad u omisión constitutiva de una infracción relevante de la presente Ley;

(c) el tamaño, el volumen de negocios anual y la cuota de mercado del operador que comete la infracción;

(c bis) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios económicos obtenidos o las pérdidas evitadas, directa o indirectamente, por la infracción;

(c bis) el grado de cooperación con las autoridades nacionales competentes, con el fin de remediar la infracción y mitigar los posibles efectos adversos de la misma;

(c ter) el grado de responsabilidad del operador, teniendo en cuenta las medidas técnicas y organizativas que haya aplicado;

(ce) la forma en que la infracción llegó a conocimiento de las autoridades nacionales competentes, en particular si el operador notificó la infracción y, en caso afirmativo, en qué medida;

(cf) el carácter intencionado o negligente de la infracción;

(cg) cualquier medida adoptada por el operador para mitigar los daños sufridos por las personas afectadas.

7. Cada Estado miembro establecerá normas sobre la medida en que podrán imponerse multas administrativas a las autoridades y organismos públicos establecidos en dicho Estado miembro.

8. Dependiendo del ordenamiento jurídico de los Estados miembros, las normas sobre multas administrativas pueden aplicarse de tal manera que las multas sean impuestas por los tribunales nacionales competentes o

otros organismos aplicables en dichos Estados miembros. La aplicación de dichas normas en esos Estados miembros tendrá un efecto equivalente.

8a. El ejercicio por parte de la autoridad de vigilancia del mercado de sus competencias en virtud del presente artículo estará sujeto a las garantías procesales apropiadas de conformidad con el Derecho de la Unión y de los Estados miembros, incluidas la tutela judicial efectiva y las garantías procesales.

8 ter. Los Estados miembros informarán anualmente a la Comisión sobre las multas administrativas que hayan impuesto durante ese año, de conformidad con el presente artículo, y sobre cualquier litigio o procedimiento judicial relacionado;

*Artículo 72*

**Multas administrativas a las instituciones, agencias y organismos de la Unión**

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, agencias y organismos de la Unión que entren en el ámbito de aplicación del presente Reglamento. A la hora de decidir si se impone una multa administrativa y de decidir el importe de la misma en cada caso concreto, se tendrán en cuenta todas las circunstancias pertinentes de la situación específica y se prestará la debida atención a lo siguiente:

(a) la naturaleza, gravedad y duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA de que se trate, así como el número de personas afectadas y el nivel de perjuicio sufrido por ellas, y cualquier infracción anterior pertinente;

(a bis) el grado de responsabilidad de la institución, agencia u organismo de la Unión, teniendo en cuenta las medidas técnicas y organizativas aplicadas por ellos;

(ab) las medidas adoptadas por la institución, agencia u organismo de la Unión para paliar los daños sufridos por las personas afectadas;

(b) el grado de cooperación con el Supervisor Europeo de Protección de Datos para remediar la infracción y mitigar los posibles efectos adversos de la misma, incluido el cumplimiento de cualquiera de las medidas previamente ordenadas por el Supervisor Europeo de Protección de Datos contra la institución, agencia u organismo de la Unión de que se trate en relación con el mismo asunto;

(c) cualquier infracción anterior similar cometida por la institución, agencia u organismo de la Unión;

(c bis) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución u organismo de la Unión notificó la infracción y, en caso afirmativo, en qué medida;

(c ter) el presupuesto anual del organismo.

2. El incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 1 500 000 euros.

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones previstos en el presente Reglamento, distintos de los establecidos en los artículos 5, estará sujeto a multas administrativas de hasta 750 000 EUR.

4. Antes de adoptar decisiones en virtud del presente artículo, el Supervisor Europeo de Protección de Datos dará a la institución, agencia u organismo de la Unión que sea objeto del procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de ser oída sobre el asunto relativo a la posible infracción. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en elementos y circunstancias sobre los que las partes afectadas hayan podido pronunciarse. Los denunciantes, si los hubiere, estarán estrechamente asociados al procedimiento.

5. En el procedimiento se respetarán plenamente los derechos de defensa de los interesados. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas o empresas en la protección de sus datos personales o secretos comerciales.

6. Los fondos recaudados mediante la imposición de multas en virtud del presente artículo contribuirán al presupuesto general de la Unión. Las multas no afectarán al funcionamiento efectivo de la institución, órgano u organismo de la Unión sancionado.

6 bis. El Supervisor Europeo de Protección de Datos notificará anualmente a la Comisión las multas administrativas que haya impuesto en virtud del presente artículo, así como cualquier litigio o procedimiento judicial.

*Artículo 72 bis*

**Multas para los proveedores de modelos de IA de uso general**

1. La Comisión puede imponer a los proveedores de modelos de IA de propósito general multas que no superen el 3% de su volumen de negocios total a nivel mundial en el ejercicio financiero anterior o 15 millones de euros, si esta cifra es superior. Las multas deberán imponerse un año después de la entrada en

aplicación de las disposiciones pertinentes del presente Reglamento con el fin de dar a los proveedores tiempo suficiente para adaptarse cuando la Comisión constate que el proveedor ha actuado de forma intencionada o negligente:

(a) infrinja las disposiciones pertinentes del presente Reglamento;

(b) no atienda una solicitud de documentación o información con arreglo al artículo 68 decies [Facultad de solicitar documentación e información], o suministro de información incorrecta, incompleta o engañosa;

(b) no cumple una medida solicitada en virtud del artículo 68 duodecies [Facultad de solicitar medidas];

(c) no ponga a disposición de la Comisión el acceso al modelo de IA de propósito general o al modelo de IA de propósito general con riesgo sistémico con vistas a realizar una evaluación con arreglo al artículo 68 undecies [Facultad de realizar evaluaciones].

Para fijar el importe de la multa o de la multa coercitiva se tendrá en cuenta la naturaleza, gravedad y duración de la infracción, así como los principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos de conformidad con el apartado 3 del artículo 68 duodecies o en los códigos de prácticas pertinentes de conformidad con el artículo 52 sexies [Códigos de prácticas].

2. Antes de adoptar la decisión con arreglo al apartado 1 del presente artículo, la Comisión comunicará sus conclusiones preliminares al proveedor del modelo de IA de propósito general o del modelo de IA de propósito general con riesgo sistémico y le dará la oportunidad de ser oído.

2 bis. Las multas impuestas de conformidad con el presente artículo deberán ser proporcionadas, disuasorias y efectivas.

2b. La información sobre las multas también se comunicará al Consejo, según proceda.

3. El Tribunal de Justicia de la Unión Europea tendrá competencia jurisdiccional plena para revisar las decisiones por las que la Comisión haya fijado una multa. Podrá anular, reducir o aumentar la multa impuesta.

4. La Comisión adoptará actos de ejecución relativos a las modalidades y disposiciones prácticas de los procedimientos con vistas a la posible adopción de decisiones de conformidad con el apartado 1. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

TÍTULO XI

# DELEGACIÓN DE PODERES Y COMITOLOGÍA

*Artículo 73*

**Ejercicio de la delegación**

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados a que se refieren [el artículo 4, el artículo 7, apartado 1, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, y el artículo 48, apartado 5] se otorgan a la Comisión por un período de cinco años a partir de ... [fecha de entrada en vigor del Reglamento].La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes a que se refieren {el apartado 1 del artículo 7, el apartado 3 del artículo 7, el apartado 3 del artículo 11, los apartados 5 y 6 del artículo 43 y el apartado 5 del artículo 48] podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de poderes que en ella se especifique. Surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Tan pronto como adopte un acto delegado, la Comisión lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del [artículo 4], del artículo 7, apartado 1, del artículo 11, apartado 3, del artículo 43, apartados 5 y 6, y del artículo 48, apartado 5, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. Este plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

*Artículo 74*

**Procedimiento de comité**

1. 1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

# TÍTULO XII DISPOSICIONES FINALES

*Artículo 75*

**Modificación del Reglamento (CE) nº 300/2008**

En el artículo 4, apartado 3, del Reglamento (CE) nº 300/2008, se añade el párrafo siguiente

" Al adoptar medidas detalladas relacionadas con las especificaciones técnicas y los procedimientos de homologación y utilización de equipos de seguridad relativos a sistemas de Inteligencia Artificial en el sentido del Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el Capítulo 2 del Título III de dicho Reglamento."

_____

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)"".

*Artículo 76*

**Modificación del Reglamento (UE) nº 167/2013**

En el artículo 17, apartado 5, del Reglamento (UE) nº 167/2013, se añade el párrafo siguiente:

" Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)".

*Artículo 77*

**Modificación del Reglamento (UE) nº 168/2013**

En el artículo 22, apartado 5, del Reglamento (UE) n.º 168/2013, se añade el párrafo siguiente: "

Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX sobre [inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

_____

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)".

*Artículo 78*

**Modificación de la Directiva 2014/90/UE**

En el artículo 8 de la Directiva 2014/90/UE, se añade el siguiente apartado: "4. Los Estados miembros velarán por que se aplique la Directiva 2014/90/UE.

"Para los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] del Parlamento Europeo y del Consejo*, al llevar a cabo sus actividades con arreglo al apartado 1 y al adoptar especificaciones técnicas y normas de ensayo de conformidad con los apartados 2 y 3, la Comisión tendrá en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)". "

_____

*Artículo 79*

**Modificación de la Directiva (UE) 2016/797**

En el artículo 5 de la Directiva (UE) 2016/797, se añade el siguiente apartado: "12.

"Al adoptar actos delegados con arreglo al apartado 1 y actos de ejecución con arreglo al apartado 11 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)".

_____"

*Artículo 80*

**Modificación del Reglamento (UE) 2018/858**

En el artículo 5 del Reglamento (UE) 2018/858 se añade el siguiente apartado: "4. En el artículo 5 del Reglamento (UE) 2018/858 se añadirá el siguiente apartado

"Al adoptar actos delegados en virtud del apartado 3 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] del Parlamento Europeo y del Consejo *, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)".

_____"

*Artículo 81*

**Modificación del Reglamento (UE) 2018/1139**

El Reglamento (UE) 2018/1139 queda modificado como sigue:

(1) En el artículo 17, se añade el apartado siguiente

"Sin perjuicio de lo dispuesto en el apartado 2, al adoptar actos de ejecución con arreglo al apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)".

En el artículo 19, se añade el párrafo siguiente:

"4. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento."

(2) En el artículo 43, se añade el apartado siguiente:

"4. Al adoptar actos de ejecución con arreglo al apartado 1 relativos a sistemas de Inteligencia Artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre Inteligencia Artificial], se tendrán en cuenta los requisitos establecidos en el Título III, Capítulo 2 de dicho Reglamento."

(3) En el artículo 47, se añade el apartado siguiente:

"3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento."

(4) En el artículo 57, se añade el apartado siguiente:

" Al adoptar los actos de ejecución relativos a los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento."

(5) En el artículo 58, se añade el párrafo siguiente:

"3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] , se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento..".

*Artículo 82*

**Modificación del Reglamento (UE) 2019/2144**

En el artículo 11 del Reglamento (UE) 2019/2144, se añade el siguiente apartado: "3. En el artículo 11 del Reglamento (UE) 2019/2144, se añadirá el siguiente apartado

"Al adoptar los actos de ejecución con arreglo al apartado 2, relativos a los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) YYY/XX [sobre inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

* Reglamento (UE) YYY/XX [sobre Inteligencia Artificial] (DO ...)..

_____"

*Artículo 82 bis*

**Directrices de la Comisión sobre la aplicación del presente Reglamento**

1. La Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre:

(a) la aplicación de los requisitos y obligaciones contemplados en los artículos 8 a 15 y en el artículo 28;

(b) las prácticas prohibidas contempladas en el artículo 5;

(c) la aplicación práctica de las disposiciones relativas a la modificación sustancial;

(d) la aplicación práctica de las obligaciones de transparencia establecidas en el artículo 52;

(e) información detallada sobre la relación del presente Reglamento con la legislación mencionada en el anexo II del presente Reglamento, así como con otros actos legislativos pertinentes de la Unión, incluso en lo que se refiere a la coherencia en su aplicación;

(f) la aplicación de la definición de sistema de IA que figura en el apartado 1 del artículo 3.

Al publicar dichas directrices, la Comisión prestará especial atención a las necesidades de las PYME, incluidas las de nueva creación, de las autoridades públicas locales y de los sectores que más puedan verse afectados por el presente Reglamento.

Las directrices a que se refiere el párrafo primero tendrán debidamente en cuenta el estado de la técnica generalmente reconocido en materia de IA, así como las normas armonizadas y especificaciones comunes pertinentes a que se refieren los artículos 40 y 41, o las normas armonizadas o especificaciones técnicas que se establezcan en virtud de la legislación de armonización de la Unión.

2. A petición de los Estados miembros o de la Oficina de AI, o por iniciativa propia, la Comisión actualizará las directrices ya adoptadas cuando lo considere necesario.

*Artículo 83*

**Sistemas de IA ya comercializados o puestos en servicio**

1. Sin perjuicio de la aplicación del artículo 5 a que se refiere el artículo 85, apartado 3 (-aa), los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en el anexo IX que se hayan comercializado o puesto en servicio antes de 12 meses después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2, deberán ajustarse al presente Reglamento antes de finales de 2030.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta en la evaluación de cada uno de los sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en el anexo IX que se lleve a cabo conforme a lo dispuesto en dichos actos respectivos y siempre que dichos actos jurídicos sean sustituidos o modificados.

2. Sin perjuicio de la aplicación del artículo 5 a que se refiere el artículo 85, apartado 3 (-aa ), el presente Reglamento se aplicará a los operadores de sistemas de IA de alto riesgo, distintos de los mencionados en el apartado 1, que hayan sido comercializados o puestos en servicio antes del [fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2], únicamente si, a partir de dicha fecha, dichos sistemas son objeto de cambios significativos en sus diseños. En el caso de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas, los proveedores e implantadores de dichos sistemas adoptarán las medidas necesarias para cumplir los requisitos del presente Reglamento cuatro años después de la fecha de entrada en vigor del mismo.

3. Los proveedores de modelos de IA de propósito general que hayan sido comercializados antes del [fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 3, letra a)] tomarán las medidas necesarias para cumplir las obligaciones establecidas en el presente Reglamento a más tardar el [2 años después de la fecha de entrada en vigor del presente Reglamento a que se refiere el artículo 85, apartado 3, letra a)].

*Artículo 84*

**Evaluación y revisión**

1. La Comisión evaluará la necesidad de modificar la lista del anexo III, la lista de prácticas de IA prohibidas del artículo 5, una vez al año tras la entrada en vigor del presente Reglamento y hasta el final del período de delegación de poderes. La Comisión presentará los resultados de dicha evaluación al Parlamento Europeo y al Consejo.

A más tardar dos años después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2, y posteriormente cada cuatro años, la Comisión evaluará e informará al Parlamento Europeo y al Consejo sobre la necesidad de modificar lo siguiente

- la necesidad de ampliar los epígrafes de zona existentes o de añadir nuevos epígrafes de zona en el anexo III;

- la lista de sistemas de IA que requieren medidas adicionales de transparencia del artículo 52;

- la eficacia del sistema de supervisión y gobernanza.

2 bis. A más tardar tres años después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 3, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Dicho informe incluirá una evaluación de la estructura de la aplicación y de la posible necesidad de crear una agencia de la Unión para resolver las deficiencias detectadas. Sobre la base de los resultados, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento. Los informes se harán públicos.

2. Los informes mencionados en el apartado 2 dedicarán una atención específica a los siguientes aspectos:

(a) la situación de los recursos financieros, técnicos y humanos de las autoridades nacionales competentes para desempeñar eficazmente las tareas que les asigna el presente Reglamento;

(b) el estado de las sanciones, y en particular de las multas administrativas contempladas en el apartado 1 del artículo 71, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento;

(b bis) las normas armonizadas adoptadas y las especificaciones comunes desarrolladas en apoyo del presente Reglamento;

(bb) el número de empresas que entran en el mercado tras la entrada en vigor del reglamento y cuántas de ellas son PYME.

3 bis. A más tardar ... [dos años después de la fecha de entrada en vigor del presente Reglamento a que se refiere el artículo 85, apartado 2], la Comisión evaluará el funcionamiento de la oficina de inteligencia artificial, si se han otorgado a la oficina poderes y competencias suficientes para cumplir sus tareas y si sería pertinente y necesario para la correcta aplicación y cumplimiento del presente Reglamento mejorar la oficina y sus competencias de ejecución y aumentar sus recursos. La Comisión presentará este informe de evaluación al Parlamento Europeo y al Consejo.

3 bis. A más tardar dos años [después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2] y, a continuación, cada cuatro años, la Comisión presentará un informe sobre la revisión de los progresos realizados en el desarrollo de productos de normalización sobre el desarrollo energéticamente eficiente de modelos de uso general y evaluará la necesidad de nuevas medidas o acciones, incluidas medidas o acciones vinculantes. El informe se presentará al Parlamento Europeo y al Consejo y se hará público.

3. En el plazo de ... [dos años a partir de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2] y, posteriormente, cada tres años, la Comisión evaluará el impacto y la eficacia de los códigos de conducta voluntarios para fomentar la aplicación de los requisitos establecidos en el título III, capítulo 2, para los sistemas de IA distintos de los sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para los sistemas de IA distintos de los sistemas de IA de alto riesgo, también en lo que se refiere a la sostenibilidad medioambiental.

4. A efectos de lo dispuesto en los apartados 1 a 4, la Junta, los Estados miembros y las autoridades nacionales competentes facilitarán a la Comisión la información que ésta solicite sin demora injustificada.

5. Al llevar a cabo las evaluaciones y revisiones a que se refieren los apartados 1 a 4, la Comisión tendrá en cuenta las posiciones y conclusiones de la Junta, del Parlamento Europeo, del Consejo y de otros organismos o fuentes pertinentes.

6. En caso necesario, la Comisión presentará propuestas adecuadas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de la tecnología, el efecto de los sistemas de IA en la salud y la seguridad, los derechos fundamentales y a la luz de los avances de la sociedad de la información.

7 bis. Para orientar las evaluaciones y revisiones mencionadas en los apartados 1 a 4 del presente artículo, la Oficina se comprometerá a desarrollar una metodología objetiva y participativa para la evaluación del nivel de riesgo basada en los criterios expuestos en los artículos pertinentes y la inclusión de nuevos sistemas en: la lista del anexo III, incluida la ampliación de los epígrafes de ámbito existentes o la adición de nuevos epígrafes de ámbito en dicho anexo; la lista de prácticas prohibidas establecida en el artículo 5; y la lista de sistemas de IA que requieren medidas de transparencia adicionales en virtud del artículo 52.

7 ter. Toda modificación del presente Reglamento con arreglo al apartado 7 del presente artículo, o los futuros actos delegados o de ejecución pertinentes, que se refieran a la legislación sectorial enumerada en el anexo II, sección B, tendrán en cuenta las especificidades reglamentarias de cada sector, así como la existencia de

mecanismos de gobernanza, evaluación de la conformidad y aplicación de la normativa y autoridades establecidas en ella.

7 quáter. A más tardar ... [cinco años a partir de la fecha de aplicación del presente Reglamento], la Comisión llevará a cabo una evaluación de la aplicación del presente Reglamento e informará de ello al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, teniendo en cuenta los primeros años de aplicación del Reglamento. Sobre la base de los resultados, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento en lo que respecta a la estructura de aplicación y a la necesidad de crear una agencia de la Unión para resolver las deficiencias detectadas.

*Artículo 85*

**Entrada en vigor y aplicación**

1. El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el Diario Oficial de la Unión Europea.

2. El presente Reglamento se aplicará a partir de [24 meses después de la entrada en vigor del Reglamento]. Por lo que respecta a la obligación a que se refiere el artículo 53, apartado 1, esta obligación incluirá bien que al menos un compartimento de regulación por Estado miembro esté operativo ese día, bien que el Estado miembro participe en el compartimento de regulación de otro Estado miembro *.

3. No obstante lo dispuesto en el apartado 2:

(-a) Los títulos I y II [Prohibiciones] se aplicarán a partir de [seis meses después de la entrada en vigor del presente Reglamento];

(a) El Capítulo 4 del Título III, el Título VI, el Título VIII bis [PAMI], el Título X [Sanciones] se aplicarán a partir del [doce meses después de la entrada en vigor del presente Reglamento];

(b) El apartado 1 del artículo 6 y las obligaciones correspondientes del presente Reglamento se aplicarán a partir de [36 meses después de la entrada en vigor del presente Reglamento].

Los códigos de prácticas estarán listos a más tardar nueve meses después de la entrada en vigor del presente Reglamento. La Oficina de AI tomará las medidas necesarias, incluida la invitación a los proveedores con arreglo al artículo 52 sexies, apartado 5.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas,

*Por el Parlamento* *EuropeoPor el Consejo*

*El* *PresidenteEl Presidente*

**ANEXO II**

## Lista de la legislación de armonización de la Unión
## Parte I

### Sección A. Lista de la legislación de armonización de la Unión basada en el nuevo marco legislativo

1. Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24) [derogada por el Reglamento sobre máquinas];

2. Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes (DO L 170 de 30.6.2009, p. 1);

3. Directiva 2013/53/UE del Parlamento Europeo y del Consejo, de 20 de noviembre de 2013, relativa a embarcaciones de recreo y motos acuáticas y por la que se deroga la Directiva 94/25/CE (DO L 354 de 28.12.2013, p. 90);

4. Directiva 2014/33/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros relativas a los ascensores y componentes de seguridad para ascensores (DO L 96 de 29.3.2014, p. 251);

5. Directiva 2014/34/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la aproximación de las legislaciones de los Estados miembros sobre los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas (DO L 96 de 29.3.2014, p. 309);

6. Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre la armonización de las legislaciones de los Estados miembros relativas a la comercialización de equipos radioeléctricos y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62);

7. Directiva 2014/68/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos a presión (DO L 189 de 27.6.2014, p. 164);

8. Reglamento (UE) 2016/424 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a las instalaciones de transporte por cable y por el que se deroga la Directiva 2000/9/CE (DO L 81 de 31.3.2016, p. 1);

Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre equipos de protección individual y por el que se deroga la Directiva 89/686/CEE del Consejo (DO L 81 de 31.3.2016, p. 51);

9. Reglamento (UE) 2016/426 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre los aparatos de gas y por el que se deroga la Directiva 2009/142/CE (DO L 81 de 31.3.2016, p. 99);

10. Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1;

11. Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios para diagnóstico in vitro y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176).

**Parte II**

**Sección B. Lista de otra legislación de armonización de la Unión**

12. Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) nº 2320/2002 (DO L 97 de 9.4.2008, p. 72).

13. Reglamento (UE) nº 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos de dos o tres ruedas y los cuatriciclos (DO L 60 de 2.3.2013, p. 52);

14. Reglamento (UE) nº 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos agrícolas y forestales (DO L 60 de 2.3.2013, p. 1);

15. Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos y por la que se deroga la Directiva 96/98/CE del Consejo (DO L 257 de 28.8.2014, p. 146);

Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea (DO L 138 de 26.5.2016, p. 44).

16. Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1);

18a. Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo para los vehículos de motor y sus remolques, y los sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, en lo que concierne a su seguridad general y a la protección de los ocupantes de vehículos y los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 78/2009, (CE) nº 79/2009 y (CE) nº 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010 de la Comisión, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012 y (UE) 2015/166 (DO L 325 de 16.12.2019, p. 1);

17. Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea y se modifican los Reglamentos (CE) n.o 2111/2005, (CE) n.o 1008/2008, (UE) n.o 996/2010, (UE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo, y por el que se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo (DO L 212 de 22.8.2018, p. 1), por lo que respecta al diseño, la producción y la comercialización de las aeronaves a que se refiere su artículo 2, apartado 1, letras a) y b), cuando se trate de aeronaves no tripuladas y de sus motores, hélices, piezas y equipos para controlarlas a distancia.

ANEXO II bis

**Lista de infracciones penales contempladas en el artículo 5, apartado 1, inciso iii)**

- terrorismo;
- trata de seres humanos;
- explotación sexual de menores y pornografía infantil;
- tráfico ilícito de estupefacientes y sustancias psicotrópicas;
- tráfico ilícito de armas, municiones y explosivos;
- asesinato, lesiones corporales graves;
- comercio ilícito de órganos y tejidos humanos;
- tráfico ilícito de materiales nucleares o radiactivos;
- secuestro, retención ilegal y toma de rehenes;
- crímenes de la competencia de la Corte Penal Internacional;
- apoderamiento ilícito de aeronaves/buques;
- violación;
- delitos contra el medio ambiente;
- robo organizado o a mano armada;
- sabotaje;
- participación en una organización delictiva implicada en uno o varios de los delitos enumerados anteriormente.

ANEXO III

**Sistemas de IA de alto riesgo contemplados en el artículo 6, apartado 2**

Los sistemas de IA de alto riesgo con arreglo al apartado 2 del artículo 6 son los sistemas de IA enumerados en cualquiera de los siguientes ámbitos:

1. Datos biométricos, en la medida en que su uso esté permitido por la legislación nacional o de la Unión pertinente:

(a) Sistemas de identificación biométrica a distancia.

Esto no incluirá los sistemas de IA destinados a ser utilizados para la verificación biométrica cuyo único propósito sea confirmar que una persona física específica es la persona que dice ser;

(aa) Sistemas de IA destinados a ser utilizados para la categorización biométrica, según atributos o características sensibles o protegidos basados en la inferencia de dichos atributos o características;

(ab) Sistemas de IA destinados al reconocimiento de emociones.

2. Infraestructuras críticas:

(a) Sistemas de IA destinados a utilizarse como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, el tráfico rodado y el suministro de agua, gas, calefacción y electricidad.

3. Educación y formación profesional:

(a) Sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión o para asignar personas físicas a instituciones educativas y de formación profesional de todos los niveles;

(b) Sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje, incluso cuando dichos resultados se utilizan para dirigir el proceso de aprendizaje de personas físicas en centros educativos y de formación profesional de todos los niveles;

(ba) Sistemas de IA destinados a ser utilizados con el fin de evaluar el nivel adecuado de educación que recibirá o al que podrá acceder un individuo, en el contexto de/en una institución de educación y formación profesional;

(bb) sistemas de IA destinados a ser utilizados para supervisar y detectar comportamientos prohibidos de los estudiantes durante las pruebas en el contexto de/en los centros de enseñanza y formación profesional.

Empleo, gestión de trabajadores y acceso al autoempleo:

(c) Sistemas de IA destinados a la contratación o selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar solicitudes de empleo y evaluar candidatos;

(d) IA destinada a utilizarse para tomar decisiones que afecten a las condiciones de las relaciones laborales, la promoción y la finalización de las relaciones contractuales laborales, para asignar tareas basadas en el comportamiento individual o en rasgos o características personales y para supervisar y evaluar el rendimiento y el comportamiento de las personas en dichas relaciones.

4. Acceso y disfrute de los servicios privados esenciales y de los servicios y prestaciones públicos esenciales:

(a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar el derecho de las personas físicas a prestaciones y servicios esenciales de asistencia pública, incluidos los servicios sanitarios, así como para conceder, reducir, revocar o reclamar dichas prestaciones y servicios;

(b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su puntuación crediticia, con la excepción de los sistemas de IA utilizados con el fin de detectar fraudes financieros;

(c) Sistemas de IA destinados a evaluar y clasificar llamadas de emergencia de personas físicas o a utilizarse para despachar o establecer prioridades en el despacho de servicios de primera respuesta de emergencia, incluidos los de policía, bomberos y ayuda médica, así como de sistemas de triaje de pacientes de atención sanitaria de emergencia;

(c bis) los sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la tarificación en relación con las personas físicas en el caso de los seguros de vida y de enfermedad.

5. Fuerzas y cuerpos de seguridad, en la medida en que su uso esté permitido por la legislación nacional o de la Unión pertinente:

(a) Sistemas de IA destinados a ser utilizados por las autoridades policiales o judiciales, o en su nombre, o por las instituciones, agencias, oficinas u organismos de la Unión en apoyo de las autoridades policiales o judiciales o en su nombre, para evaluar el riesgo de que una persona física sea víctima de infracciones penales;

Sistemas de IA destinados a ser utilizados por o en nombre de las autoridades policiales o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades policiales como polígrafos y herramientas similares;

(d) Sistemas de IA destinados a ser utilizados por las autoridades policiales y judiciales o en su nombre, o por instituciones, agencias, oficinas u organismos de la Unión en apoyo de las autoridades policiales y judiciales para evaluar la fiabilidad de las pruebas en el curso de la investigación o el enjuiciamiento de delitos;

(e) Sistemas de IA destinados a ser utilizados por las fuerzas y cuerpos de seguridad o en su nombre o por instituciones, agencias, oficinas u organismos de la Unión en apoyo de las fuerzas y cuerpos de seguridad para evaluar el riesgo de una persona física de delinquir o reincidir no basados únicamente en la elaboración de perfiles de personas físicas a que se refiere el artículo 3, apartado 4, de la Directiva (UE) 2016/680 o para evaluar rasgos y características de personalidad o comportamientos delictivos anteriores de personas físicas o grupos;

(f) Sistemas de IA destinados a ser utilizados por o en nombre de las autoridades policiales o por agencias de la Unión instituciones, agencias, oficinas u organismos en apoyo de las autoridades policiales para la elaboración de perfiles de personas físicas a que se refiere el artículo 3, apartado 4, de la Directiva (UE) 2016/680 en el curso de la detección, investigación o enjuiciamiento de infracciones penales.

6. Gestión de la migración, el asilo y el control de fronteras, en la medida en que su uso esté permitido por la legislación nacional o de la Unión pertinente:

(a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes como polígrafos y herramientas similares;

(b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o por los órganos u organismos de la Unión, o en su nombre, para evaluar un riesgo, incluido un riesgo de seguridad, un riesgo de migración irregular o un riesgo sanitario, planteado por una persona física que pretenda entrar o haya entrado en el territorio de un Estado miembro;

(d) los sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o por sus representantes o por los organismos de la Unión para asistir a las autoridades públicas competentes en el examen de las solicitudes de asilo, visado y permisos de residencia y las reclamaciones conexas en relación con la admisibilidad de las personas físicas que solicitan un estatuto, incluida la evaluación conexa de la fiabilidad de las pruebas;

(d bis) los sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, incluidas las agencias, oficinas u organismos de la Unión, o en su nombre, en el contexto de la gestión de la migración, el asilo y el control de fronteras, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje.

7. Administración de justicia y procesos democráticos:

(a) Sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para asistir a una autoridad judicial en la investigación e interpretación de hechos y de la ley y en la aplicación de la ley a un conjunto concreto de hechos o utilizados de forma similar en la resolución alternativa de litigios;

(aa) Sistemas de **IA destinados** a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento de voto de personas físicas en el ejercicio de su voto en elecciones o referendos. No se incluyen los sistemas de IA a cuyos resultados no están expuestas directamente las personas físicas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico.

ANEXO IV

**Documentación técnica contemplada en el apartado 1 del artículo 11**

La documentación técnica a que se refiere el apartado 1 del artículo 11 contendrá como mínimo la siguiente información, según proceda para el sistema de IA pertinente:

1. Descripción general del sistema de IA:

(a) su finalidad, el nombre del proveedor y la versión del sistema que refleje su relación con versiones anteriores;

(b) el modo en que el sistema de IA interactúa o puede utilizarse para interactuar con hardware o software, incluidos otros sistemas de IA, que no formen parte del propio sistema de IA, cuando proceda;

(c) las versiones de software o firmware pertinentes y cualquier requisito relacionado con la actualización de versiones;

(d) la descripción de todas las formas en que el sistema de IA se comercializa o se pone en servicio (por ejemplo, paquete de software integrado en hardware, descargable, API, etc.);

(e) la descripción del hardware en el que está previsto que se ejecute el sistema de IA;

(f) cuando el sistema de IA sea un componente de productos, fotografías o ilustraciones que muestren las características externas, el marcado y la disposición interna de dichos productos;

(fa) una descripción básica de la interfaz de usuario proporcionada al desplegador;

(g) instrucciones de uso para el desplegador y una descripción básica de la interfaz de usuario proporcionada al desplegador, en su caso.

2. Una descripción detallada de los elementos del sistema de IA y del proceso para su desarrollo, incluyendo:

(a) los métodos y pasos seguidos para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas preentrenados proporcionados por terceros y la forma en que éstos han sido utilizados, integrados o modificados por el proveedor;

(b) las especificaciones de diseño del sistema, es decir, la lógica general del sistema de IA y de los algoritmos; las principales opciones de diseño, incluidos los fundamentos y las hipótesis adoptadas, también en relación con las personas o grupos de personas sobre los que se basa el sistema

que se pretende utilizar; las principales opciones de clasificación; para qué se ha diseñado el sistema y la importancia de los diferentes parámetros; la descripción de la producción esperada y la calidad de la producción del sistema; las decisiones sobre cualquier posible compensación realizada en relación con las soluciones técnicas adoptadas para cumplir los requisitos establecidos en el Capítulo 2 del Título III;

(c) la descripción de la arquitectura del sistema, explicando cómo los componentes de software se apoyan o alimentan entre sí y se integran en el procesamiento global; los recursos informáticos utilizados para desarrollar, entrenar, probar y validar el sistema de IA;

(d) cuando proceda, los requisitos de datos en términos de fichas técnicas que describan las metodologías y técnicas de formación y los conjuntos de datos de formación utilizados, incluida una descripción general de estos conjuntos de datos, información sobre su procedencia, alcance y características principales; cómo se obtuvieron y seleccionaron los datos; procedimientos de etiquetado (por ejemplo, para el aprendizaje supervisado), metodologías de limpieza de datos (por ejemplo, detección de valores atípicos);

(e) evaluación de las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluida una evaluación de las medidas técnicas necesarias para facilitar la interpretación de los resultados de los sistemas de IA por parte de quienes los despliegan, de conformidad con el artículo 13, apartado 3, letra d);

(f) en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su rendimiento, junto con toda la información pertinente relacionada con las soluciones técnicas adoptadas para garantizar la conformidad continua del sistema de IA con los requisitos pertinentes establecidos en el capítulo 2 del título III;

(g) los procedimientos de validación y ensayo utilizados, incluida la información sobre los datos de validación y ensayo utilizados y sus principales características; los parámetros utilizados para medir la precisión, la solidez y el cumplimiento de otros requisitos pertinentes establecidos en el título III, capítulo 2, así como los impactos potencialmente discriminatorios; los registros de ensayo y todos los informes de ensayo fechados y firmados por las personas responsables, incluso en lo que respecta a los cambios predeterminados a que se refiere la letra f);

(ga) medidas de ciberseguridad implantadas.

3. Información detallada sobre la supervisión, el funcionamiento y el control del sistema de IA, en particular en lo que se refiere a: sus capacidades y limitaciones de rendimiento, incluidos los grados de precisión para personas o grupos de personas específicos sobre los que se aplica el sistema.

que se pretende utilizar y el nivel general de precisión esperado en relación con su finalidad prevista; los resultados imprevistos previsibles y las fuentes de riesgos para la salud y la seguridad, los derechos fundamentales y la discriminación en vista de la finalidad prevista del sistema de IA; las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de los sistemas de IA por parte de quienes los despliegan; las especificaciones sobre los datos de entrada, según proceda;

3. Una descripción de la idoneidad de las métricas de rendimiento para el sistema de IA específico;

4. Una descripción detallada del sistema de gestión de riesgos de conformidad con el artículo 9;

5. Una descripción de los cambios relevantes realizados por el proveedor en el sistema a lo largo de su ciclo de vida;

6. Una lista de las normas armonizadas aplicadas total o parcialmente cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea; cuando no se hayan aplicado tales normas armonizadas, una descripción detallada de las soluciones adoptadas para cumplir los requisitos establecidos en el capítulo 2 del título III, incluida una lista de otras normas y especificaciones técnicas pertinentes aplicadas;

7. Una copia de la declaración de conformidad de la UE;

8. Una descripción detallada del sistema establecido para evaluar el rendimiento del sistema de IA en la fase posterior a la comercialización de conformidad con el artículo 61, incluido el plan de seguimiento posterior a la comercialización mencionado en el apartado 3 del artículo 61.

ANEXO V

**Declaración de conformidad de la UE**

La declaración UE de conformidad a que se refiere el artículo 48 contendrá toda la información siguiente:

1. Nombre y tipo del sistema de IA y cualquier referencia adicional inequívoca que permita la identificación y trazabilidad del sistema de IA;

2. Nombre y dirección del proveedor o, en su caso, de su representante autorizado;

3. Una declaración de que la declaración UE de conformidad se expide bajo la exclusiva responsabilidad del proveedor;

4. Una declaración de que el sistema de IA en cuestión es conforme con el presente Reglamento y, si procede, con cualquier otra legislación pertinente de la Unión que prevea la expedición de una declaración UE de conformidad;

4 bis. Cuando un sistema de IA implique el tratamiento de datos personales, una declaración de que dicho sistema de IA cumple los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680;

5. Referencias a cualquier norma armonizada pertinente utilizada o a cualquier otra especificación común en relación con la cual se declare la conformidad;

6. En su caso, nombre y número de identificación del organismo notificado, descripción del procedimiento de evaluación de la conformidad realizado e identificación del certificado expedido;

7. Lugar y fecha de emisión de la declaración, nombre y cargo de la persona que la firmó, así como una indicación de por quién y en nombre de quién firmó, firma.

ANEXO VI

**Procedimiento de evaluación de la conformidad basado en el control interno**

1. El procedimiento de evaluación de la conformidad basado en el control interno es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 4.

2. El proveedor verifica que el sistema de gestión de la calidad establecido cumple los requisitos del artículo 17.

3. El proveedor examina la información contenida en la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos en el capítulo 2 del título III.

4. El proveedor también verifica que el proceso de diseño y desarrollo del sistema de IA y su seguimiento postcomercialización, tal como se menciona en el artículo 61, son coherentes con la documentación técnica.

ANEXO VII

**Conformidad basada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica**

1. Introducción

La conformidad basada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 5.

2. Visión general

El sistema de gestión de la calidad aprobado para el diseño, desarrollo y ensayo de sistemas de IA con arreglo al artículo 17 se examinará de conformidad con el punto 3 y se someterá a la vigilancia especificada en el punto 5. La documentación técnica del sistema de IA se examinará de conformidad con el punto 4.

3. Sistema de gestión de la calidad

3.1. La solicitud del proveedor deberá incluir:

(a) el nombre y la dirección del prestador y, si la solicitud la presenta el representante autorizado, también su nombre y dirección;

(b) la lista de sistemas de IA cubiertos por el mismo sistema de gestión de la calidad;

(c) la documentación técnica de cada sistema de IA incluido en el mismo sistema de gestión de la calidad;

(d) la documentación relativa al sistema de gestión de la calidad, que abarcará todos los aspectos enumerados en el artículo 17;

(e) una descripción de los procedimientos establecidos para garantizar que el sistema de gestión de la calidad sigue siendo adecuado y eficaz;

(f) una declaración escrita de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de gestión de la calidad será evaluado por el organismo notificado, que determinará si cumple los requisitos contemplados en el artículo 17.

La decisión se notificará al prestador o a su representante autorizado.

La notificación incluirá las conclusiones de la evaluación del sistema de gestión de la calidad y la decisión de evaluación motivada.

3.3. El sistema de gestión de la calidad aprobado deberá seguir siendo aplicado y mantenido por el proveedor para que siga siendo adecuado y eficaz.

3.4. El proveedor comunicará al organismo notificado cualquier modificación prevista del sistema de gestión de la calidad aprobado o de la lista de sistemas de gestión de la calidad cubiertos por éste.

Las modificaciones propuestas serán examinadas por el organismo notificado, que decidirá si el sistema de gestión de la calidad modificado sigue cumpliendo los requisitos contemplados en el punto 3.2 o si es necesaria una nueva evaluación.

El organismo notificado notificará su decisión al proveedor. La notificación contendrá las conclusiones del examen de los cambios y la decisión de evaluación motivada.

4. Control de la documentación técnica

4.1. Además de la solicitud contemplada en el punto 3, el proveedor presentará una solicitud ante un organismo notificado de su elección para la evaluación de la documentación técnica relativa al sistema de IA que tenga previsto comercializar o poner en servicio y que esté cubierto por el sistema de gestión de la calidad contemplado en el punto 3.

4.2. La solicitud deberá incluir:

(a) el nombre y la dirección del proveedor;

(b) una declaración escrita de que no se ha presentado la misma solicitud ante ningún otro organismo notificado;

(c) la documentación técnica mencionada en el Anexo IV.

4.3. El organismo notificado examinará la documentación técnica. Cuando proceda, y limitado a lo necesario para el desempeño de sus tareas, se concederá al organismo notificado pleno acceso a los conjuntos de datos de formación, validación y ensayo utilizados, incluso, cuando proceda y con sujeción a las salvaguardias de seguridad, a través de interfaces de programación de aplicaciones (API) u otros medios técnicos y herramientas pertinentes que permitan el acceso a distancia.

4.4. Al examinar la documentación técnica, el organismo notificado podrá exigir que el proveedor aporte más pruebas o realice más ensayos para poder evaluar adecuadamente la conformidad del sistema de IA con los requisitos establecidos en el capítulo 2 del título III.

Siempre que el organismo notificado no esté satisfecho con los ensayos realizados por el proveedor, el organismo notificado realizará directamente los ensayos adecuados, según proceda.

4.5. Cuando sea necesario para evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el título III, capítulo 2, después de que se hayan agotado todos los demás medios razonables para verificar la conformidad y hayan resultado insuficientes, y previa solicitud motivada, también se concederá al organismo notificado acceso a los modelos de formación y entrenamiento del sistema de IA, incluidos sus parámetros pertinentes. Dicho acceso estará sujeto al Derecho de la Unión vigente en materia de protección de la propiedad intelectual y de los secretos comerciales.

4.6. La decisión se notificará al proveedor o a su representante autorizado. La notificación contendrá las conclusiones de la evaluación de la documentación técnica y la decisión de evaluación motivada.

Cuando el sistema de IA sea conforme con los requisitos establecidos en el capítulo 2 del título III, el organismo notificado expedirá un certificado UE de evaluación de la documentación técnica. El certificado indicará el nombre y la dirección del proveedor, las conclusiones del examen, las condiciones (en su caso) de validez y los datos necesarios para la identificación del sistema de IA.

El certificado y sus anexos contendrán toda la información pertinente que permita evaluar la conformidad del sistema de IA y, en su caso, controlar el sistema de IA durante su utilización.

En caso de que el sistema de IA no sea conforme con los requisitos establecidos en el capítulo 2 del título III, el organismo notificado se negará a expedir un certificado UE de evaluación de la documentación técnica e informará de ello al solicitante, explicando detalladamente su negativa.

Cuando el sistema de IA no cumpla el requisito relativo a los datos utilizados para entrenarlo, será necesario volver a entrenarlo antes de solicitar una nueva evaluación de la conformidad. En este caso, la decisión de evaluación motivada del organismo notificado por la que se deniegue la expedición del certificado UE de evaluación de la documentación técnica contendrá consideraciones específicas sobre los datos de calidad utilizados para entrenar el sistema de IA, en particular sobre los motivos del incumplimiento.

4.7. Cualquier modificación del sistema de IA que pueda afectar a la conformidad del sistema de IA con los requisitos o a su finalidad prevista deberá ser aprobada por el organismo notificado que haya expedido

el certificado UE de evaluación de la documentación técnica. El proveedor informará a dicho organismo notificado de su intención de introducir cualquiera de los cambios mencionados o si tiene conocimiento de que se van a producir. Los cambios previstos serán evaluados por el organismo notificado, que decidirá si requieren una nueva evaluación de la conformidad con arreglo al artículo 43, apartado 4, o si pueden abordarse mediante un suplemento del certificado UE de evaluación de la documentación técnica. En este último caso, el organismo notificado evaluará los cambios, notificará su decisión al proveedor y, si se aprueban los cambios, expedirá al proveedor un suplemento del certificado UE de evaluación de la documentación técnica.

5. Vigilancia del sistema de gestión de la calidad aprobado

5.1. El objetivo de la vigilancia efectuada por el organismo notificado mencionado en el punto 3 es cerciorarse de que el proveedor cumple debidamente las condiciones del sistema de gestión de la calidad aprobado.

5.2. A efectos de evaluación, el proveedor permitirá al organismo notificado acceder a los locales en los que se lleven a cabo el diseño, el desarrollo y los ensayos de los sistemas de IA. Además, el proveedor compartirá con el organismo notificado toda la información necesaria.

5.3. El organismo notificado efectuará auditorías periódicas para cerciorarse de que el proveedor mantiene y aplica el sistema de gestión de la calidad y facilitará al proveedor un informe de la auditoría. En el contexto de dichas auditorías, el organismo notificado podrá realizar ensayos adicionales de los sistemas de IA para los que se haya expedido un certificado UE de evaluación de la documentación técnica.

## ANEXO VIII

**Información que debe presentarse en el momento del registro de los sistemas de IA de alto riesgo de conformidad con el artículo 51**

**SECCIÓN A - Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el apartado 1 del artículo 51**

En relación con los sistemas de IA de alto riesgo que deban registrarse de conformidad con el artículo 51, apartado 1, se facilitará la siguiente información, que se mantendrá actualizada posteriormente:

1. Nombre, dirección y datos de contacto del proveedor;

2. Cuando la presentación de la información la realice otra persona en nombre del proveedor, el nombre, la dirección y los datos de contacto de dicha persona;

3. Nombre, dirección y datos de contacto del representante autorizado, si procede;

4. Nombre comercial del sistema de IA y cualquier referencia adicional inequívoca que permita la identificación y trazabilidad del sistema de IA;

5. Descripción de la finalidad prevista del sistema de IA y de los componentes y funciones soportados a través de este sistema de IA;

5a. Una descripción básica y concisa de la información utilizada por el sistema (datos, entradas) y su lógica de funcionamiento;

6. Estado del sistema de IA (comercializado o en servicio; ya no comercializado/en servicio, retirado);

7. Tipo, número y fecha de caducidad del certificado expedido por el organismo notificado y nombre o número de identificación de dicho organismo notificado, en su caso;

8. Una copia escaneada del certificado mencionado en el punto 7, cuando proceda;

9. Estados miembros en los que el sistema de IA se comercializa o ha sido comercializado, puesto en servicio o puesto a disposición en la Unión;

10. Una copia de la declaración UE de conformidad mencionada en el artículo 48;

11. Instrucciones electrónicas de uso; esta información no se facilitará para los sistemas de IA de alto riesgo en los ámbitos de la aplicación de la ley y la gestión de la migración, el asilo y el control fronterizo a que se refieren los puntos 1, 6 y 7 del anexo III.

URL para información adicional (opcional).

**SECCIÓN B - Información que deben presentar los implantadores de sistemas de IA de alto riesgo de conformidad con el artículo 51, apartado 1 ter**

Se facilitará la siguiente información y, posteriormente, se mantendrá actualizada en relación con los sistemas de IA de alto riesgo que deban registrarse de conformidad con el artículo 51:

1. El nombre, la dirección y los datos de contacto del responsable de la implantación;

2. El nombre, la dirección y los datos de contacto de la persona que presenta la información en nombre del remitente;

5. Un resumen de las conclusiones de la evaluación de impacto sobre los derechos fundamentales realizada de conformidad con el artículo 29 bis;

6. La URL de la entrada del sistema de IA en la base de datos de la UE por su proveedor;

7. Un resumen de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, tal como se especifica en el artículo 29, apartado 6, del presente Reglamento, cuando proceda.

**SECCIÓN C - Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el apartado 1 bis del artículo 51**

En relación con los sistemas de IA que deban registrarse de conformidad con el artículo 51, apartado 1 bis, se facilitará la siguiente información, que posteriormente se mantendrá actualizada.

1. Nombre, dirección y datos de contacto del proveedor;

1. Cuando la presentación de la información la realice otra persona en nombre del proveedor, el nombre, la dirección y los datos de contacto de dicha persona;

2. Nombre, dirección y datos de contacto del representante autorizado, si procede;

3. Nombre comercial del sistema de IA y cualquier referencia adicional inequívoca que permita la identificación y trazabilidad del sistema de IA;

4. Descripción de la finalidad prevista del sistema de IA;

En base a qué criterio o criterios previstos en el apartado 2 bis del artículo 6 se considera que el sistema de IA no es de alto riesgo;

5. Breve resumen de los motivos para considerar que el sistema de IA no es de alto riesgo en aplicación del procedimiento del apartado 2 bis del artículo 6;

6. Situación del sistema de IA (en el mercado, o en servicio; ya no comercializado/en servicio, retirado); Estados miembros en los que el sistema de IA se comercializa o se ha comercializado, se ha puesto en servicio o se ha comercializado en la Unión.

ANEXO VIII bis

**Información que debe presentarse al registrar los sistemas ai de alto riesgo enumerados en el anexo iii en relación con los ensayos en condiciones reales de conformidad con el artículo 54 bis**

Se facilitará la siguiente información, que posteriormente se mantendrá actualizada, en relación con los ensayos en condiciones reales que se registrarán de conformidad con el artículo 54 bis:

1. Número de identificación único para toda la Unión de las pruebas en condiciones reales;

2. Nombre y datos de contacto del proveedor o posible proveedor y de los usuarios que participan en las pruebas en condiciones reales;

3. Breve descripción del sistema de IA, su finalidad prevista y demás información necesaria para la identificación del sistema;

4. Resumen de las principales características del plan de pruebas en condiciones reales;

5. Información sobre la suspensión o finalización de las pruebas en condiciones reales.

ANEXO IX

**Legislación de la Unión sobre sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia**

1. Sistema de Información de Schengen

(a) Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al uso del Sistema de Información de Schengen para el retorno de los nacionales de terceros países en situación irregular (DO L 312 de 7.12.2018, p. 1).

(b) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de los controles fronterizos, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y por el que se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L 312 de 7.12.2018, p. 14).

(c) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo y por el que se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

2. Sistema de Información de Visados

(a) Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DE EL CONSEJO por el que se modifican el Reglamento (CE) n.º 767/2008, el Reglamento (CE) n.º 810/2009, el Reglamento (UE) 2017/2226, el Reglamento (UE) 2016/399, el Reglamento XX/2018 [Reglamento de interoperabilidad] y la Decisión 2004/512/CE y se deroga la Decisión 2008/633/JAI del Consejo - COM(2018) 302 final. Se actualizará una vez que los colegisladores adopten el Reglamento (abril/mayo de 2021).

3. Eurodac

(a) Propuesta modificada de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema "Eurodac" para la comparación de datos biométricos con vistas a la aplicación efectiva del Reglamento (UE) XXX/XXX [Reglamento sobre la gestión del asilo y la migración] y del Reglamento (UE) XXX/XXX [Reglamento sobre reasentamiento], para la identificación de un tercero en situación irregular-.

nacional de un país o apátrida y sobre las solicitudes de comparación con los datos de Eurodac por parte de las autoridades policiales de los Estados miembros y Europol con fines policiales, y por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) 2019/818 - COM(2020) 614 final.

4. Sistema de entrada/salida

(a) Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y los datos de denegación de entrada de los nacionales de terceros países que cruzan las fronteras exteriores de los Estados miembros y por el que se determinan las condiciones de acceso al SES a efectos de la aplicación de la ley, y por el que se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011 (DO L 327 de 9.12.2017, p. 20).

5. Sistema Europeo de Información y Autorización de Viajes

(a) Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (ETIAS) y se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226 (DO L 236 de 19.9.2018, p. 1).

(b) Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con el fin de establecer un Sistema Europeo de Información y Autorización de Viajes (ETIAS) (DO L 236 de 19.9.2018, p. 72).

6. Sistema europeo de información de antecedentes penales sobre nacionales de terceros países y apátridas

(a) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado de identificación de los Estados miembros que poseen información sobre condenas penales para nacionales de terceros países y apátridas (ECRIS-TCN) como complemento del sistema de información europeo de antecedentes penales y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

7. Interoperabilidad

Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco de interoperabilidad entre los sistemas de información de la UE en el ámbito de las fronteras y los visados (DO L 135 de 22.5.2019, p. 27).

(a) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración (DO L 135 de 22.5.2019, p. 85).

**ANEXO IX bis**

**Documentación técnica contemplada en el artículo 52 quater, apartado 1 bis: documentación técnica para proveedores de modelos de IA de uso general:**

**Sección 1: Información que deben facilitar todos los proveedores de modelos de IA de propósito general**

La documentación técnica a que se refiere la letra b) del artículo X contendrá como mínimo la siguiente información, en función del tamaño y el perfil de riesgo del modelo:

1. Una descripción general del modelo de IA de propósito general que incluye:

(a) las tareas que debe realizar el modelo y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;

(b) políticas de uso aceptable aplicables;

(c) la fecha de publicación y los métodos de distribución;

(d) la arquitectura y el número de parámetros;

(e) modalidad (por ejemplo, texto, imagen) y formato de las entradas y salidas;

(f) la licencia.

2. Una descripción detallada de los elementos del modelo a que se refiere el apartado 1, e información pertinente del proceso de elaboración, incluida la siguientes elementos:

(a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para que el modelo de IA de propósito general se integre en los sistemas de IA;

(b) las especificaciones de diseño del modelo y del proceso de formación, incluidas las metodologías y técnicas de formación, las opciones clave de diseño, incluidos los fundamentos y las suposiciones realizadas; para qué se ha diseñado el modelo con el fin de optimizarlo y la relevancia de los distintos parámetros, según proceda;

(c) información sobre los datos utilizados para la formación, las pruebas y la validación, en su caso, incluido el tipo y la procedencia de los datos y las metodologías de conservación (por ejemplo, limpieza, filtrado, etc.), el número de puntos de datos, su alcance y sus principales características; cómo se ha utilizado la

se obtuvieron y seleccionaron los datos, así como todas las demás medidas para detectar la inadecuación de las fuentes de datos y los métodos para detectar sesgos identificables, en su caso;

(d) los recursos informáticos utilizados para entrenar el modelo (por ejemplo, número de operaciones en coma flotante - FLOPs), tiempo de entrenamiento y otros detalles relevantes relacionados con el entrenamiento;

(e) consumo de energía conocido o estimado del modelo; en caso de no conocerse, podría basarse en información sobre los recursos computacionales utilizados ;

**Sección 2: Información adicional que deben facilitar los proveedores de modelos de IA de propósito general con riesgo sistémico**

3. Descripción detallada de las estrategias de evaluación, incluidos los resultados de la evaluación, sobre la base de los protocolos y herramientas de evaluación públicos disponibles o, en su defecto, de otras metodologías de evaluación. Las estrategias de evaluación incluirán criterios de evaluación, métricas y la metodología sobre la identificación de limitaciones.

4. En su caso, descripción detallada de las medidas aplicadas con el fin de realizar pruebas adversativas internas y/o externas (por ejemplo, red teaming), adaptaciones de modelos, incluida la alineación y el ajuste.

5. En su caso, descripción detallada de la arquitectura del sistema que explique cómo los componentes de software se construyen o alimentan entre sí y se integran en el procesamiento global.

ANEXO IX ter

**Información sobre transparencia contemplada en el artículo 52 quater, apartado 1 ter: documentación técnica para proveedores de modelos de IA de propósito general a proveedores posteriores que integren el modelo en su sistema de IA.**

La información a que se refiere el artículo 52 quater contendrá, como mínimo, lo siguiente:

1. Una descripción general del modelo de IA de propósito general que incluye:

(a) las tareas que debe realizar el modelo y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;

(b) políticas de uso aceptable aplicables;

(c) la fecha de publicación y los métodos de distribución;

(d) el modo en que el modelo interactúa o puede utilizarse para interactuar con hardware o software que no forme parte del propio modelo, en su caso;

(e) las versiones de los programas informáticos pertinentes relacionados con el uso del modelo de IA de propósito general, en su caso;

(f) arquitectura y número de parámetros,

(g) modalidad (por ejemplo, texto, imagen) y formato de las entradas y salidas;

(h) la licencia del modelo.

2. Una descripción de los elementos del modelo y del proceso para su desarrollo, incluyendo:

(a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para que el modelo de IA de propósito general se integre en los sistemas de IA;

(b) modalidad (por ejemplo, texto, imagen, etc.) y formato de las entradas y salidas y su tamaño máximo (por ejemplo, longitud de la ventana de contexto, etc.);

(c) información sobre los datos utilizados para la formación, las pruebas y la validación, en su caso, incluidos el tipo y la procedencia de los datos y las metodologías de conservación.

**Criterios para la designación de modelos de IA de propósito general con riesgo sistémico a que se refiere el artículo 52 bis**

Para determinar que un modelo de IA de propósito general tiene capacidades o repercusiones equivalentes a las de las letras a) y b) del artículo 52 bis, la Comisión tendrá en cuenta los siguientes criterios:

(a) número de parámetros del modelo;

(b) calidad o tamaño del conjunto de datos, por ejemplo, medido a través de tokens;

(c) la cantidad de cálculo utilizada para entrenar el modelo, medida en FLOPs o indicada por una combinación de otras variables como el coste estimado del entrenamiento, el tiempo estimado necesario para el entrenamiento o el consumo de energía estimado para el entrenamiento;

(d) modalidades de entrada y salida del modelo, como texto a texto (grandes modelos lingüísticos), texto a imagen, multimodalidad, y los umbrales del estado de la técnica para determinar las capacidades de alto impacto para cada modalidad, y el tipo específico de entradas y salidas (por ejemplo, secuencias biológicas);

(e) Puntos de referencia y evaluaciones de las capacidades del modelo, teniendo en cuenta el número de tareas sin formación adicional, la adaptabilidad para aprender tareas nuevas y distintas, su grado de autonomía y escalabilidad, las herramientas a las que tiene acceso;

(f) tiene un gran impacto en el mercado interior debido a su alcance, que se presumirá cuando se haya puesto a disposición de al menos 10 000 usuarios empresariales registrados establecidos en la Unión;

(g) número de usuarios finales registrados.