COMISIÓN
EUROPEA

Bruselas, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

1.1. Razones y objetivos de la propuesta

La presente exposición de motivos acompaña a la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). La inteligencia artificial (IA) es un conjunto de tecnologías de rápida evolución que puede generar un amplio abanico de beneficios económicos y sociales en todos los sectores y las actividades sociales. Mediante la mejora de la predicción, la optimización de las operaciones y de la asignación de los recursos y la personalización de la prestación de servicios, la inteligencia artificial puede facilitar la consecución de resultados positivos desde el punto de vista social y medioambiental, así como proporcionar ventajas competitivas esenciales a las empresas y la economía europea. Esto es especialmente necesario en sectores de gran impacto como el cambio climático, el medio ambiente y la salud, el sector público, las finanzas, la movilidad, los asuntos internos y la agricultura. No obstante, los mismos elementos y técnicas que potencian los beneficios socioeconómicos de la IA también pueden dar lugar a nuevos riesgos o consecuencias negativas para personas concretas o la sociedad en su conjunto. En vista de la velocidad a la que cambia la tecnología y las dificultades que podrían surgir, la UE está decidida a buscar un enfoque equilibrado. Redunda en interés de la Unión preservar su liderazgo tecnológico y garantizar que los europeos puedan aprovechar nuevas tecnologías que se desarrollen y funcionen de acuerdo con los valores, los derechos fundamentales y los principios de la UE.

Esta propuesta responde al compromiso político de la Presidenta Von der Leyen, que en sus orientaciones políticas para la Comisión 2019-2024, tituladas «Una Unión que se esfuerza por lograr más resultados»[1], anunció que la Comisión presentaría propuestas de legislación para un enfoque europeo coordinado sobre las implicaciones éticas y humanas de la IA. Tras dicho anuncio, el 19 de febrero de 2020 la Comisión publicó el Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza[2]. En el Libro Blanco se definen las opciones existentes para alcanzar el doble objetivo de promover la adopción de la IA y de abordar los riesgos vinculados a determinados usos de esta nueva tecnología. La presente propuesta pretende alcanzar el segundo objetivo para desarrollar un ecosistema de confianza mediante la proposición de un marco jurídico destinado a lograr que la IA sea fiable. La propuesta se basa en los valores y derechos fundamentales de la UE y tiene por objeto inspirar confianza en los ciudadanos y otros usuarios para que adopten soluciones basadas en la IA, al tiempo que trata de animar a las empresas a que desarrollen este tipo de soluciones. La IA debe ser un instrumento para las personas y una fuerza positiva en la sociedad, y su fin último debe ser incrementar el bienestar humano. En consecuencia, las normas relativas a la IA presente en el mercado de la Unión o que afecte de algún modo a sus habitantes deben estar centradas en las personas, a fin de que la población tenga la seguridad de que la tecnología se usa de un modo seguro y en consonancia con la ley, lo que también implica respetar los derechos fundamentales. Tras la publicación del Libro Blanco, la Comisión inició una amplia consulta con las partes interesadas, muchas de las cuales la acogieron con gran interés y defendieron con ahínco la intervención reguladora para hacer frente a los desafíos y las preocupaciones que entraña el uso cada vez mayor de la IA.

---

1 https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_es_0.pdf.

2 Comisión Europea, *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza*, COM (2020) 65 final, 2020.

La propuesta responde asimismo a peticiones explícitas del Parlamento Europeo (PE) y el Consejo Europeo, que han solicitado en repetidas ocasiones que se adopten medidas legislativas para garantizar el buen funcionamiento del mercado interior de los sistemas de inteligencia artificial (en adelante, «sistemas de IA») y que en la Unión se aborden apropiadamente las ventajas y los riesgos que conlleva la IA. Respalda el objetivo de que la Unión sea un líder mundial en el desarrollo de inteligencia artificial segura, digna de confianza y ética, como indicó el Consejo Europeo[3], y garantiza la protección de los principios éticos, como solicitó específicamente el Parlamento Europeo[4].

En 2017, el Consejo Europeo instó a «concienciarse de la urgencia de hacer frente a las nuevas tendencias, lo que comprende cuestiones como la inteligencia artificial [...], garantizando al mismo tiempo un elevado nivel de protección de los datos, así como los derechos digitales y las normas éticas»[5]. En sus Conclusiones de 2019 relativas al Plan Coordinado sobre la Inteligencia Artificial[6], el Consejo de la Unión Europea destacó la importancia de garantizar el pleno respeto de los derechos de los ciudadanos europeos y pidió que se revisase la legislación pertinente en vigor con vistas a garantizar su adaptación a las nuevas oportunidades y retos que plantea la IA. Asimismo, el Consejo Europeo ha pedido que se defina con claridad qué usos de la IA deben considerarse de alto riesgo[7].

Las Conclusiones más recientes, del 21 de octubre de 2020, instaban además a afrontar la opacidad, la complejidad, el sesgo, cierto grado de imprevisibilidad y un comportamiento parcialmente autónomo de ciertos sistemas de IA, para garantizar su compatibilidad con los derechos fundamentales y facilitar la aplicación de las normas jurídicas[8].

El Parlamento Europeo también ha llevado a cabo una gran labor en el ámbito de la IA. En octubre de 2020, aprobó una serie de resoluciones relativas a la IA sobre cuestiones como la ética[9], la responsabilidad civil[10] y los derechos de propiedad intelectual[11]. En 2021, a estas les siguieron diversas resoluciones sobre el uso de la IA en el ámbito penal[12] y en los sectores educativo, cultural y audiovisual[13]. La Resolución del PE sobre un marco de los aspectos

---

3 Consejo Europeo, Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) – Conclusiones, EUCO 13/20, 2020, p. 6.

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

5 Consejo Europeo, *Reunión del Consejo Europeo (19 de octubre de 2017) – Conclusiones* EUCO 14/17, 2017, p. 8.

6 Consejo de la Unión Europea, *Inteligencia artificial: b) Conclusiones relativas al Plan Coordinado sobre la Inteligencia Artificial – Adopción*, 6177/19, 2019.

7 Consejo Europeo, *Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) – Conclusiones*, EUCO 13/20, 2020.

8 Consejo de la Unión Europea, *Conclusiones de la Presidencia - La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital*, 11481/20, 2020.

9 Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012(INL).

10 Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre un régimen de responsabilidad civil en materia de inteligencia artificial, 2020/2014(INL).

11 Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial, 2020/2015(INI).

12 Proyecto de informe del Parlamento Europeo sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales, 2020/2016(INI).

13 Proyecto de informe del Parlamento Europeo sobre la inteligencia artificial en los sectores educativo, cultural y audiovisual, 2020/2017(INI). En ese sentido, la Comisión ha aprobado el Plan de Acción de Educación Digital 2021-2027: Adaptar la educación y la formación a la era digital, que prevé el desarrollo de unas directrices éticas sobre IA y el uso de los datos en la educación. Comunicación de la Comisión COM(2020) 624 final.

éticos de la inteligencia artificial, la robótica y las tecnologías conexas recomienda específicamente a la Comisión que proponga medidas legislativas para aprovechar las oportunidades y los beneficios de la IA, sin dejar de garantizar la protección de los principios éticos. La Resolución incluye el texto para una propuesta legislativa de Reglamento sobre principios éticos para el desarrollo, la implementación y el uso de la inteligencia artificial, la robótica y las tecnologías conexas. De conformidad con el compromiso político asumido por la Presidenta Von der Leyen en sus orientaciones políticas en lo que respecta a las resoluciones adoptadas por el Parlamento Europeo en virtud del artículo 225 del TFUE, la presente propuesta tiene en cuenta la citada Resolución del Parlamento Europeo, respetando plenamente los principios de proporcionalidad, subsidiariedad y mejora de la legislación.

En este contexto político, la Comisión propone un marco reglamentario sobre inteligencia artificial con los siguientes **objetivos específicos**:

- garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;
- garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;
- mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;
- facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.

Para alcanzar dichos objetivos, la presente propuesta presenta un enfoque normativo horizontal, equilibrado y proporcionado, para la IA, que se limita a establecer los requisitos mínimos necesarios para subsanar los riesgos y problemas vinculados a la IA, sin obstaculizar ni impedir indebidamente el desarrollo tecnológico y sin aumentar de un modo desproporcionado el coste de introducir soluciones de IA en el mercado. La propuesta establece un marco jurídico sólido y flexible. Por un lado, las opciones reglamentarias fundamentales que plantea, incluidos los requisitos basados en principios que deben cumplir los sistemas de IA, son amplias y pueden resistir el paso del tiempo. Por otro lado, establece un sistema regulatorio proporcionado centrado en un enfoque normativo basado en los riesgos y claramente definido que no impone restricciones innecesarias al comercio, en el que la intervención jurídica se adapta a aquellas situaciones concretas en las que existe un motivo de preocupación justificado o en las que es posible anticipar razonablemente que se producirá un problema en un futuro próximo. Al mismo tiempo, el marco jurídico incluye mecanismos flexibles que le permiten adaptarse de manera dinámica a medida que evoluciona la tecnología y surgen nuevas situaciones preocupantes.

La propuesta establece normas armonizadas para el desarrollo, la introducción en el mercado y la utilización de sistemas de IA en la Unión a partir de un enfoque proporcionado basado en los riesgos. También propone una definición única de la IA que puede resistir el paso del tiempo. Asimismo, prohíbe determinadas prácticas particularmente perjudiciales de IA por ir en contra de los valores de la Unión y propone restricciones y salvaguardias específicas en relación con determinados usos de los sistemas de identificación biométrica remota con fines de aplicación de la ley. La propuesta establece una sólida metodología de gestión de riesgos para definir aquellos sistemas de IA que plantean un «alto riesgo» para la salud y la seguridad o los derechos fundamentales de las personas. Dichos sistemas de IA tendrán que cumplir una serie de requisitos horizontales obligatorios que garanticen su fiabilidad y ser sometidos a procedimientos de evaluación de la conformidad antes de poder introducirse en el mercado de

la Unión. Del mismo modo, se imponen obligaciones previsibles, proporcionadas y claras a los proveedores y los usuarios de dichos sistemas, con el fin de garantizar la seguridad y el respeto de la legislación vigente protegiendo los derechos fundamentales durante todo el ciclo de vida de los sistemas de IA. En el caso de determinados sistemas de IA, solo se proponen obligaciones mínimas en materia de transparencia, en particular cuando se utilizan robots conversacionales o ultrafalsificaciones.

Las normas propuestas se aplicarán mediante un sistema de gobernanza a escala de los Estados miembros, el cual aprovechará las estructuras ya existentes, y también por medio de un mecanismo de cooperación a escala de la Unión con el que se establecerá un Comité Europeo de Inteligencia Artificial. Además, se proponen medidas adicionales para impulsar la innovación, en particular a través de espacios controlados de pruebas para la IA y otras medidas encaminadas a reducir la carga normativa y a respaldar a las pequeñas y medianas empresas (pymes) y las empresas emergentes.

1.2. Coherencia con las disposiciones existentes en la misma política sectorial

Debido a su carácter horizontal, la propuesta debe ser plenamente coherente con la legislación de la Unión vigente aplicable a los sectores donde ya se utilizan o es probable que se utilicen en un futuro próximo sistemas de IA de alto riesgo.

También está garantizada su coherencia con la Carta de los Derechos Fundamentales de la Unión Europea y el Derecho derivado de la Unión vigente en materia de protección de datos, protección de los consumidores, no discriminación e igualdad de género. La propuesta debe entenderse sin perjuicio del Reglamento General de Protección de Datos [Reglamento (UE) 2016/679] y la Directiva sobre protección de datos en el ámbito penal [Directiva (UE) 2016/680], a los que complementa con un conjunto de normas armonizadas aplicables al diseño, el desarrollo y la utilización de determinados sistemas de IA de alto riesgo y con restricciones de determinados usos de los sistemas de identificación biométrica remota. Asimismo, la propuesta complementa el Derecho de la Unión vigente en materia de no discriminación al establecer requisitos específicos que tienen por objeto reducir al mínimo el riesgo de discriminación algorítmica, en particular en lo tocante al diseño y la calidad de los conjuntos de datos empleados para desarrollar sistemas de IA, los cuales van acompañados de obligaciones referentes a la realización de pruebas, la gestión de riesgos, la documentación y la vigilancia humana durante todo el ciclo de vida de tales sistemas. La propuesta debe entenderse sin perjuicio de la aplicación de las disposiciones del Derecho de la Unión en materia de competencia.

En cuanto a los sistemas de IA de alto riesgo que son componentes de seguridad de productos, esta propuesta se integrará en la legislación sectorial vigente en materia de seguridad para garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales. En particular, en el caso de los sistemas de IA de alto riesgo asociados a productos cubiertos por la legislación del nuevo marco legislativo (p. ej., máquinas, productos sanitarios, juguetes), los requisitos que establece la presente propuesta para los sistemas de IA se comprobarán como parte de los procedimientos de evaluación de la conformidad previstos en la legislación pertinente del nuevo marco legislativo. En cuanto a la interrelación de múltiples requisitos, aunque la idea es que los estipulados en la presente propuesta cubran los riesgos de seguridad específicos de los sistemas de IA, la legislación del nuevo marco legislativo busca garantizar la seguridad general del producto final, por lo que podría contener requisitos específicos relativos a la integración segura de un sistema de IA en el producto final. La propuesta de un Reglamento relativo a las máquinas, que se aprueba el mismo día que la presente propuesta, refleja plenamente este enfoque. La presente propuesta no se aplicaría directamente a los sistemas de IA de alto riesgo asociados a productos cubiertos por la legislación «de antiguo

enfoque» pertinente (p. ej., aviación o automóviles). No obstante, cuando se apruebe legislación de aplicación o delegada en virtud de dichos actos legislativos, se deberán tener en cuenta los requisitos esenciales *ex ante* aplicables a los sistemas de IA de alto riesgo establecidos en esta propuesta.

En cuanto a los sistemas de IA facilitados o utilizados por entidades de crédito reguladas, procede designar a las autoridades responsables de supervisar la legislación de la Unión relativa a los servicios financieros como autoridades competentes para controlar los requisitos estipulados en la presente propuesta, a fin de garantizar el cumplimiento coherente de las obligaciones previstas en ella y en la legislación de la Unión relativa a los servicios financieros en aquellos casos en que los sistemas de IA están, en cierta medida, regulados implícitamente en relación con el sistema de gobernanza interna de las entidades de crédito. En aras de mejorar la coherencia, el procedimiento de evaluación de la conformidad y algunas de las obligaciones procedimentales de los proveedores previstas en la presente propuesta se integran en los procedimientos contemplados en la Directiva 2013/36/UE relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial[14].

Esta propuesta también es coherente con la legislación de la Unión aplicable en materia de servicios, incluida la relativa a los servicios de intermediarios regulados por la Directiva 2000/31/CE sobre el comercio electrónico[15] y la reciente propuesta de la Comisión para una Ley de Servicios Digitales[16].

Con respecto a los sistemas de IA que son componentes de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia gestionado por la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud (eu-LISA), la propuesta no se aplicará a aquellos sistemas de IA que se introduzcan en el mercado o se pongan en servicio antes de que transcurra un año desde la fecha de aplicación del presente Reglamento, a menos que la sustitución o modificación de dichos actos legislativos redunde en un cambio significativo en el diseño o la finalidad prevista del sistema o los sistemas de IA de que se trate.

1.3. Coherencia con otras políticas de la Unión

Esta propuesta forma parte de un paquete integral más amplio de medidas que abordan los problemas derivados del desarrollo y la utilización de la IA, los cuales se examinan en el *Libro Blanco sobre la inteligencia artificial*. Por consiguiente, quedan garantizadas la coherencia y la complementariedad con otras iniciativas de la Comisión en curso o previstas que también buscan solucionar estos problemas, tales como la revisión de la legislación sectorial sobre determinados productos (p. ej., la Directiva sobre máquinas o la Directiva relativa a la seguridad general de los productos) e iniciativas que abordan los problemas de responsabilidad vinculados a las nuevas tecnologías y, en particular, a los sistemas de IA. Dichas iniciativas se fundamentarán en la presente propuesta y la complementarán, con miras

---

[14] 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 (Texto pertinente a efectos del EEE) (DO L 176 de 27.6.2013, p. 338).

[15] 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).

[16] Véase la propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE [COM(2020) 825].

a aportar claridad jurídica y a impulsar el desarrollo de un ecosistema de confianza en la IA en Europa.

La propuesta también es coherente con la estrategia digital general de la Comisión en su contribución para promover una tecnología al servicio de las personas, uno de los tres pilares principales de las orientaciones políticas y los objetivos anunciados en la Comunicación titulada «Configurar el futuro digital de Europa»[17]. En este sentido, establece un marco coherente, efectivo y proporcionado destinado a garantizar que la IA se desarrolle de modos que respeten los derechos de las personas y se ganen su confianza, con el fin de lograr una Europa adaptada a la era digital y convertir los próximos diez años en la **Década Digital**[18].

Además, la promoción de la innovación impulsada por la IA está estrechamente vinculada a la **Ley de Gobernanza de Datos**[19], la **Directiva relativa a los datos abiertos**[20] y otras iniciativas emprendidas en el marco de la **Estrategia de Datos de la UE**[21], que establecerán mecanismos y servicios de confianza para reutilizar, compartir y poner en común datos esenciales para el desarrollo de modelos de IA de gran calidad basados en datos.

La propuesta también fortalece de manera considerable el papel de la UE como ayuda a conformar las normas globales y promover una IA fiable que esté en consonancia con los valores e intereses de la Unión. Además, proporciona a la Unión unos sólidos cimientos para un diálogo de mayor calado con sus socios externos, en particular con terceros países, y en foros internacionales sobre cuestiones relacionadas con la IA.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

2.1. Base jurídica

La base jurídica de la propuesta es, en primer lugar, el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que trata de la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior.

Esta propuesta constituye una parte fundamental de la Estrategia para el Mercado Único Digital de la UE. Su objetivo primordial es garantizar el correcto funcionamiento del mercado interior mediante el establecimiento de normas armonizadas, en particular en lo que respecta al desarrollo, la introducción en el mercado de la Unión y el uso de productos y servicios que empleen tecnologías de IA o se suministren como sistemas de IA independientes. Algunos Estados miembros ya están estudiando normas nacionales destinadas a garantizar que la IA sea segura y se desarrolle y utilice de conformidad con las obligaciones asociadas a los derechos fundamentales. Es probable que esto ocasione dos problemas fundamentales: i) la fragmentación del mercado interno en lo que respecta a elementos esenciales, en particular los requisitos aplicables a los productos y servicios de IA, su comercialización, su utilización, y la responsabilidad y supervisión de las autoridades públicas; y ii) la disminución considerable de la seguridad jurídica de los proveedores y usuarios de sistemas de IA en lo tocante a cómo se

---

17 Comunicación de la Comisión «Configurar el futuro digital de Europa» [COM(2020) 67 final].

18 2030 Digital Compass: the European way for the Digital Decade (Brújula Digital para 2030: la Vía Europea de la Década Digital).

19 Propuesta de Reglamento relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), COM(2020)767.

20 Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, PE/28/2019/REV/1 (DO L 172 de 26.6.2019, p. 56).

21 Comunicación de la Comisión «Una Estrategia Europea de Datos» [COM(2020) 66 final].

aplicarán a dichos sistemas las normas vigentes y nuevas en la Unión. Habida cuenta de la amplia circulación transfronteriza de productos y servicios, la mejor manera de solucionar estos dos problemas es mediante legislación de armonización de la UE.

De hecho, en la propuesta se definen los requisitos obligatorios comunes aplicables al diseño y el desarrollo de determinados sistemas de IA antes de su introducción en el mercado, los cuales se pondrán posteriormente en práctica por medio de unas normas técnicas armonizadas. La propuesta también tiene en cuenta la situación una vez que los sistemas de IA se han introducido en el mercado, pues armoniza la manera en que se llevan a cabo los controles *ex post*.

Además, dado que la presente propuesta contiene determinadas normas específicas para la protección de las personas en relación con el tratamiento de los datos personales, fundamentalmente restricciones del uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, resulta adecuado basar este Reglamento, en lo que atañe a dichas normas específicas, en el artículo 16 del TFUE.

2.2. Subsidiariedad (en el caso de competencia no exclusiva)

La naturaleza de la IA, que a menudo depende de conjuntos de datos amplios y variados y que puede integrarse en cualquier producto o servicio que circula libremente por el mercado interior, implica que los Estados miembros no pueden alcanzar de manera efectiva los objetivos de esta propuesta por sí solos. Asimismo, está surgiendo un mosaico de normas nacionales con posibles divergencias que entorpecerá la circulación fluida en la UE de productos y servicios asociados a sistemas de IA y no garantizará de manera efectiva la seguridad y la protección de los derechos fundamentales y los valores de la Unión en los distintos Estados miembros. Las estrategias nacionales orientadas a afrontar estos problemas solo crearán inseguridad jurídica y barreras adicionales, y ralentizarán la adopción de la IA por parte del mercado.

Resultará más fácil alcanzar los objetivos de esta propuesta a escala de la Unión para evitar que el mercado único se fragmente en marcos nacionales potencialmente contradictorios que impidan la libre circulación de bienes y servicios que lleven IA incorporada. Por otro lado, el establecimiento de un marco reglamentario europeo sólido para conseguir que la IA sea fiable garantizará la igualdad de condiciones y protegerá a todas las personas, al tiempo que reforzará la competitividad y la base industrial de Europa en el ámbito de la IA. Además, la única manera de proteger la soberanía digital de la UE y de aprovechar sus herramientas y competencias reguladoras para crear normas y reglas globales es mediante la adopción de medidas comunes a escala de la Unión.

2.3. Proporcionalidad

La propuesta se fundamenta en los marcos jurídicos existentes y es proporcionada y necesaria para alcanzar sus objetivos, ya que sigue un enfoque basado en los riesgos y únicamente impone cargas normativas cuando es probable que un sistema de IA entrañe altos riesgos para los derechos fundamentales y la seguridad. A los demás sistemas de IA que no son de alto riesgo tan solo se les imponen obligaciones muy limitadas en materia de transparencia; por ejemplo, en lo que se refiere a la presentación de información para comunicar el uso de un sistema de IA cuando este interactúe con humanos. En el caso de los sistemas de IA de alto riesgo, los requisitos relativos a los datos de alta calidad, la documentación y la trazabilidad, la transparencia, la vigilancia humana, la precisión y la solidez son estrictamente necesarios para reducir los riesgos de la IA para los derechos fundamentales y la seguridad y que no están cubiertos por otros marcos jurídicos existentes. Unas normas armonizadas, y los

instrumentos de orientación y cumplimiento en que se apoyan, ayudarán a los proveedores y los usuarios a cumplir los requisitos establecidos en la propuesta y a reducir al mínimo sus gastos. Los costes en que incurren los operadores son proporcionales a los objetivos logrados y a los beneficios que pueden obtener gracias a esta propuesta en términos económicos y de reputación.

2.4. Elección del instrumento

Si se ha elegido el Reglamento como instrumento jurídico, es por la necesidad de aplicar uniformemente las nuevas normas, tales como la definición de IA, la prohibición de determinadas prácticas perjudiciales que la IA permitiría y la clasificación de determinados sistemas de IA. Puesto que, de conformidad con el artículo 288 del TFUE, los reglamentos son directamente aplicables, la elección de este instrumento reducirá la fragmentación jurídica y facilitará el desarrollo de un mercado único de sistemas de IA legales, seguros y fiables. En particular, lo hará mediante la introducción de un conjunto armonizado de requisitos básicos relativos a los sistemas de IA considerados de alto riesgo, así como obligaciones aplicables a los proveedores y usuarios de dichos sistemas; la mejora de la protección de los derechos fundamentales, y la aportación de seguridad jurídica tanto para los operadores como para los consumidores.

Al mismo tiempo, las disposiciones del Reglamento no son excesivamente prescriptivas y permiten que los Estados miembros actúen a distintos niveles en relación con aquellos elementos que no socavan los objetivos de la iniciativa, en particular en lo que respecta a la organización interna del sistema de vigilancia del mercado y la adopción de medidas para promover la innovación.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, LAS CONSULTAS CON LAS PARTES INTERESADAS Y LAS EVALUACIONES DE IMPACTO

3.1. Consulta con las partes interesadas

La presente propuesta es el resultado de una amplia consulta con todas las principales partes interesadas, la cual se atuvo a los principios generales y las normas mínimas de consulta de la Comisión a las partes interesadas.

El 19 de febrero de 2020, el mismo día que se publicó el *Libro Blanco sobre la inteligencia artificial*, se inició una **consulta pública en línea**, que se prolongó hasta el 14 de junio de 2020. Su objetivo era recabar observaciones y opiniones sobre el Libro Blanco. La consulta estaba dirigida a todas las partes interesadas de los sectores público y privado, incluidos los gobiernos, las autoridades locales, las organizaciones comerciales y de otra índole, los interlocutores sociales, los expertos, los académicos y los ciudadanos. Tras analizar todas las respuestas recibidas, la Comisión publicó un resumen de resultados y las respuestas individuales en su sitio web[22].

En total se recibieron 1 215 contribuciones, de las cuales 352 procedieron de empresas u organizaciones o asociaciones comerciales, 406 de particulares (el 92 % de ellos, de la UE), 152 de representantes de instituciones académicas o de investigación, y 73 de autoridades públicas. Asimismo, 160 encuestados representaban a la sociedad civil (en concreto, 9 organizaciones de consumidores, 129 organizaciones no gubernamentales y 22 sindicatos), y 72 se adscribieron a la categoría «Otros». De los 352 representantes de la empresa y la industria, 222 representaban a empresas y negocios. El 41,5 % de estos eran microempresas,

[22] Puede ver aquí todos los resultados de la consulta.

pequeñas y medianas empresas, mientras que el resto eran asociaciones comerciales. En total, el 84 % de las respuestas de empresas e industrias procedieron de la EU-27. Dependiendo de la pregunta, entre 81 y 598 de los encuestados utilizaron la opción de texto libre para añadir comentarios. Se presentaron más de 450 documentos de posición a través del sitio web de EU Survey, bien para aportar información adicional a las respuestas del cuestionario (más de 400), o bien como contribuciones independientes (más de 50).

En términos generales, las partes interesadas coinciden en la necesidad de tomar medidas. Una gran mayoría cree que existen lagunas legislativas o que se requiere una nueva legislación. No obstante, varias partes interesadas advirtieron a la Comisión de la necesidad de evitar duplicidades, obligaciones contradictorias y la sobrerregulación. Numerosos comentarios insistieron en la importancia de adoptar un marco reglamentario proporcionado y tecnológicamente neutro.

Las partes interesadas solicitaron fundamentalmente una definición ajustada, clara y precisa de la IA. Asimismo, señalaron que, además de aclarar el término «inteligencia artificial», es importante definir conceptos como «riesgo», «alto riesgo», «bajo riesgo», «identificación biométrica remota» y «perjuicio».

La mayoría de los encuestados está explícitamente a favor del enfoque basado en el riesgo. Se consideró que un marco basado en riesgos era una opción mejor que un Reglamento que cubra todos los sistemas de IA. Los tipos de riesgos y amenazas deben basarse en un planteamiento sector por sector y caso por caso. Asimismo, los riesgos deben calcularse teniendo en cuenta su repercusión para los derechos y la seguridad.

Los espacios controlados de pruebas podrían resultar muy útiles para promover la IA, y algunas partes interesadas, en especial las asociaciones comerciales, los consideran una buena opción.

Más del 50 % de los encuestados que dieron su opinión sobre los modelos de aplicación, en especial los pertenecientes a asociaciones comerciales, se mostraron a favor de combinar una autoevaluación de riesgos *ex ante* con la supervisión *ex post* en el caso de los sistemas de IA de alto riesgo.

3.2. Obtención y uso de asesoramiento especializado

La propuesta se sustenta en dos años de análisis y estrecha colaboración de las partes interesadas, entre las que figuran académicos, empresas, interlocutores sociales, organizaciones no gubernamentales, Estados miembros y ciudadanos. El trabajo preparatorio comenzó en 2018 con la creación de un **grupo de expertos de alto nivel sobre IA**, con una composición amplia e inclusiva. En concreto, estaba integrado por cincuenta y dos expertos reconocidos cuya misión era asesorar a la Comisión sobre la aplicación de la Estrategia sobre Inteligencia Artificial de la propia Comisión. En abril de 2019, la Comisión respaldó[23] los requisitos clave establecidos en las directrices éticas para una IA fiable[24] de dicho grupo de expertos, los cuales se habían revisado para tener en cuenta las más de quinientas contribuciones presentadas por las partes interesadas. Dichos requisitos clave son el reflejo de la idea generalizada y común, como demuestra el amplio abanico de códigos y principios éticos desarrollados por multitud de organizaciones privadas y públicas en Europa y otros lugares, de que el desarrollo y la utilización de la IA deben guiarse por determinados principios esenciales orientados a los valores. La lista de evaluación para una inteligencia

[23] Comisión Europea, *Generar confianza en la inteligencia artificial centrada en el ser humano* [COM(2019) 168].

[24] Grupo de expertos de alto nivel sobre inteligencia artificial, *Directrices éticas para una IA fiable*, 2019.

artificial fiable[25] hizo efectivos dichos requisitos en un proceso de prueba en el que participaron más de trescientas cincuenta organizaciones.

Asimismo, se constituyó la **Alianza de la IA**[26], una plataforma donde unas cuatro mil partes interesadas celebran debates sobre las implicaciones tecnológicas y sociales de la IA, los cuales culminan con la celebración de una asamblea anual en la materia.

El **Libro Blanco** sobre la IA profundizó más en este enfoque inclusivo, lo que animó a más de 1 250 partes interesadas a formular comentarios y a presentar más de 450 documentos de posición adicionales. En consecuencia, la Comisión publicó una evaluación inicial de impacto que, a su vez, dio lugar a más de 130 comentarios[27]. También se organizaron **otros talleres y eventos con las partes interesadas**, en cuyos resultados se fundamenta el análisis de la evaluación de impacto y las opciones que se plantean en la presente propuesta[28]. Asimismo, se encargó un **estudio externo** destinado a su utilización como material para la evaluación de impacto.

3.3. Evaluación de impacto

En consonancia con su política de «legislar mejor», la Comisión sometió la presente propuesta a una evaluación de impacto que fue examinada por su Comité de Control Reglamentario. El 16 de diciembre de 2020 se celebró una reunión con dicho Comité, que al término de esta emitió un dictamen negativo. No obstante, el 21 de marzo de 2021, después de que la evaluación de impacto fuera revisada en profundidad para abordar los comentarios recibidos y volviera a presentarse, el Comité de Control Reglamentario emitió un dictamen favorable. Los dictámenes del Comité de Control Reglamentario, las recomendaciones y una explicación de cómo se han tenido en cuenta figuran en el anexo 1 de la evaluación de impacto.

La Comisión examinó diversas opciones para alcanzar el objetivo general de la propuesta, que es **garantizar el buen funcionamiento del mercado único** mediante la creación de las condiciones necesarias para el desarrollo y la utilización de una IA fiable en la Unión.

Se evaluaron cuatro opciones con distintos grados de intervención reguladora:

- **Opción 1**: un instrumento legislativo de la UE que establezca un régimen voluntario de etiquetado.
- **Opción 2**: una estrategia sectorial *ad hoc*.
- **Opción 3**: un instrumento legislativo horizontal de la UE que se apoye en un enfoque proporcionado basado en los riesgos.

---

25 Grupo de expertos de alto nivel sobre inteligencia artificial, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment* (*Lista de evaluación para una inteligencia artificial fiable con fines de autoevaluación*), 2020.

26 La Alianza de la IA es un foro de múltiples interesados que se creó en junio de 2018. Para más información, véase el siguiente enlace: https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

27 Comisión Europea, *Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence*(Evaluación inicial de impacto para una propuesta de acto legislativo del Parlamento Europeo y del Consejo que establezca los requisitos para la inteligencia artificial).

28 Para conocer los detalles de todas las consultas que se han llevado a cabo, véase el anexo 2 de la evaluación de impacto.

- **Opción 3+:** un instrumento legislativo horizontal de la UE que se apoye en un enfoque proporcionado basado en los riesgos + códigos de conducta para los sistemas de IA que no sean de alto riesgo.
- **Opción 4**: un instrumento legislativo horizontal de la UE que establezca requisitos obligatorios para todos los sistemas de IA, con independencia del riesgo que conlleven.

Conforme a la metodología establecida por la Comisión, se evaluó cada opción atendiendo a sus repercusiones económicas y sociales, prestando especial atención a su impacto para los derechos fundamentales. La opción preferida es la opción 3+, un marco regulatorio que únicamente se aplique a los sistemas de IA de alto riesgo, con la posibilidad de que todos los proveedores de sistemas de IA que no sean de alto riesgo sigan un código de conducta. Los requisitos se referirán a los datos, la documentación y la trazabilidad; la comunicación de información y la transparencia; la vigilancia humana, y la solidez y la precisión, y serían de obligado cumplimiento para los sistemas de IA de alto riesgo. Las empresas podrían introducir códigos de conducta para otros sistemas de IA de forma voluntaria.

Se consideró que la opción preferida era adecuada para responder de la manera más eficaz a los objetivos de la presente propuesta. Al exigir que los desarrolladores y usuarios de IA adopten una serie de medidas limitadas pero efectivas, la opción preferida contribuye a reducir el riesgo de que se vulneren los derechos fundamentales y se ponga en peligro la seguridad de las personas, al tiempo que fomenta la supervisión y el cumplimiento efectivos, pues centra los requisitos únicamente en los sistemas en los que el riesgo de que se produzcan tales violaciones es elevado. En consecuencia, dicha opción reduce al mínimo los costes de cumplimiento, evitando así que la adopción se ralentice innecesariamente debido a unos precios y costes de cumplimiento más elevados. Al objeto de evitar las posibles desventajas para las pymes, esta opción incluye varias disposiciones que facilitan el cumplimiento de los requisitos correspondientes y reducen sus costes. Entre otras cosas, estas disposiciones prevén la creación de espacios controlados de pruebas y establecen la obligación de tener en cuenta los intereses de las pymes cuando se fijen las tarifas asociadas a la evaluación de la conformidad.

La opción preferida incrementará la confianza de la población en la IA, brindará una mayor seguridad jurídica a las empresas, y hará que los Estados miembros dejen de tener motivos para adoptar medidas unilaterales que podrían fragmentar el mercado único. El incremento de la demanda debido al aumento de la confianza, la mayor cantidad de ofertas disponibles gracias a la seguridad jurídica y la ausencia de obstáculos para la circulación transfronteriza de sistemas de IA harán, con toda probabilidad, que el mercado único para la IA florezca. La Unión Europea continuará desarrollando un ecosistema de IA de rápido crecimiento de servicios y productos innovadores con tecnología de IA integrada o sistemas de IA independientes, el cual redundará en el aumento de la autonomía digital.

Las empresas o las autoridades públicas que desarrollen o utilicen aplicaciones de IA que entrañen un riesgo elevado para la seguridad o los derechos fundamentales de los ciudadanos tendrían que cumplir requisitos y obligaciones específicos. El cumplimiento de estos requisitos tendría un coste aproximado de entre 6 000 y 7 000 EUR para el suministro de un sistema de IA de alto riesgo promedio con un valor de en torno a 170 000 EUR para 2025. Por su parte, los usuarios de la IA tendrían que cubrir, cuando correspondiese, el coste anual del tiempo dedicado a garantizar la vigilancia humana, en función del uso concreto que hagan. Se calcula que este coste ascendería a entre 5 000 y 8 000 EUR al año, aproximadamente. Además, los proveedores de IA de alto riesgo podrían tener que abonar unos costes de verificación adicionales de entre 3 000 y 7 500 EUR. Las empresas o las autoridades públicas

que desarrollen o utilicen aplicaciones de IA no consideradas de alto riesgo únicamente tendrían que cumplir unas obligaciones mínimas de información. No obstante, podrían decidir unirse a otras y, juntas, adoptar un código de conducta para cumplir los requisitos adecuados y garantizar la fiabilidad de sus sistemas de IA. En tal caso, los costes podrían ser, como máximo, tan elevados como los de los sistemas de IA de alto riesgo, aunque lo más probable es que fueran inferiores.

Las repercusiones de las opciones para las distintas categorías de partes interesadas (operadores económicos o empresas; organismos de evaluación de la conformidad, organismos de normalización y otros organismos públicos; particulares o ciudadanos; e investigadores) se explican en detalle en el anexo 3 de la evaluación de impacto en que se fundamenta la presente propuesta.

3.4. Adecuación y simplificación de la normativa

La presente propuesta define las obligaciones que se aplicarán a los proveedores y usuarios de los sistemas de IA de alto riesgo. Para los proveedores que desarrollen dichos sistemas y los introduzcan en el mercado de la Unión, generará seguridad jurídica y garantizará que no surja ningún obstáculo para el suministro transfronterizo de servicios y productos asociados a la IA. En el caso de las empresas que utilizan la IA, fomentará la confianza entre sus clientes. En cuanto a las administraciones públicas, favorecerá que la población confíe en el uso de la IA y reforzará los mecanismos de cumplimiento al introducir un mecanismo de coordinación europeo, contemplar las capacidades adecuadas y facilitar que se realicen auditorías de los sistemas de IA con nuevos requisitos en materia de documentación, trazabilidad y transparencia. Asimismo, el marco contemplará medidas específicas en favor de la innovación, tales como espacios controlados de pruebas y medidas concretas que ayuden a los usuarios y proveedores de sistemas de IA de alto riesgo a pequeña escala a cumplir las nuevas normas.

Asimismo, la propuesta tiene el objetivo específico de reforzar la competitividad y la base industrial de Europa en el ámbito de la IA. Está garantizada su plena armonización con la legislación sectorial vigente en la Unión aplicable a los sistemas de IA (p. ej., en relación con determinados productos y servicios), lo que aportará más claridad y simplificará el cumplimiento de las nuevas normas.

3.5. Derechos fundamentales

El uso de la IA, con sus características particulares (p. ej., la opacidad, la complejidad, la dependencia de datos, el comportamiento autónomo) puede tener repercusiones negativas para múltiples derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»). La presente propuesta pretende garantizar un elevado nivel de protección para dichos derechos fundamentales, así como hacer frente a diversas fuentes de riesgo mediante un enfoque basado en los riesgos claramente definido. Sirviéndose de un conjunto de requisitos destinados a conseguir que la IA sea fiable y que se impongan obligaciones proporcionadas a todos los participantes en la cadena de valor, la propuesta reforzará y promoverá la protección de los derechos salvaguardados por la Carta: el derecho a la dignidad humana (artículo 1), el respeto de la vida privada y familiar y la protección de datos de carácter personal (artículos 7 y 8), la no discriminación (artículo 21) y la igualdad entre hombres y mujeres (artículo 23). Su objetivo es evitar un efecto paralizante sobre los derechos a la libertad de expresión (artículo 11) y de reunión (artículo 12), y garantizar el derecho a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia y los derechos de la defensa (artículos 47 y 48), así como el principio general de buena administración. Asimismo, al ser aplicable en determinados ámbitos, la propuesta tendrá efectos positivos en los derechos de diversos grupos especiales, como los derechos de los

trabajadores a unas condiciones de trabajo justas y equitativas (artículo 31), un elevado nivel de protección de los consumidores (artículo 28), los derechos del niño (artículo 24) y la integración de las personas discapacitadas (artículo 26). El derecho a un nivel elevado de protección del medio ambiente y la mejora de su calidad (artículo 37) también es pertinente, en particular en lo que respecta a la salud y la seguridad de las personas. Además, las obligaciones relativas a la realización de pruebas *ex ante*, la gestión de riesgos y la vigilancia humana facilitarán el respeto de otros derechos fundamentales, ya que contribuirán a reducir al mínimo el riesgo de adoptar decisiones asistidas por IA erróneas o sesgadas en esferas críticas como la educación y la formación, el empleo, servicios importantes, la aplicación de la ley y el poder judicial. En caso de que se sigan produciendo violaciones de los derechos fundamentales, la transparencia y la trazabilidad garantizadas de los sistemas de IA, unidas a unos controles *ex post* sólidos, permitirán ofrecer a las personas afectadas una compensación efectiva.

La presente propuesta impone ciertas restricciones a la libertad de empresa (artículo 16) y la libertad de las artes y de las ciencias (artículo 13), con vistas a garantizar que se respeten los fines imperiosos de interés general relacionados con ámbitos como la salud, la seguridad, la protección de los consumidores y la protección de otros derechos fundamentales («innovación responsable») cuando se desarrolle y utilice tecnología de IA de alto riesgo. Dichas restricciones son proporcionadas y se limitan al mínimo necesario para prevenir y reducir riesgos graves para la seguridad y violaciones probables de los derechos fundamentales.

Las obligaciones que exigen una mayor transparencia tampoco afectarán de manera desproporcionada al derecho a la protección de la propiedad intelectual (artículo 17, apartado 2), puesto que únicamente se aplicarán a la información mínima necesaria para que las personas ejerzan su derecho a una compensación efectiva y solo exigirán la transparencia necesaria hacia las autoridades de supervisión y las encargadas de la aplicación de la ley, conforme a sus respectivos mandatos. La información se divulgará siempre con arreglo a la legislación pertinente en la materia, entre la que se incluye 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. Cuando las autoridades públicas y los organismos notificados deban tener acceso a información confidencial o al código fuente para examinar el cumplimiento de las obligaciones sustanciales, tendrán que cumplir obligaciones de confidencialidad vinculantes.

4. REPERCUSIONES PRESUPUESTARIAS

Los Estados miembros tendrán que designar autoridades de supervisión encargadas de aplicar los requisitos legislativos. Su función de supervisión podría apoyarse en los mecanismos existentes, por ejemplo, en lo que respecta a los organismos de evaluación de la conformidad o la vigilancia del mercado, pero requeriría unos conocimientos tecnológicos y unos recursos humanos y financieros suficientes. En función de la estructura que exista previamente en cada Estado miembro, estos podrían ascender a entre uno y veinticinco equivalentes a jornada completa por Estado miembro.

El «estado financiero» adjunto a la presente propuesta ofrece un resumen detallado de los costes implicados.

5. OTROS ELEMENTOS

5.1. Planes de ejecución y modalidades de seguimiento, evaluación e información

Resulta esencial establecer un mecanismo sólido de seguimiento y evaluación para garantizar que la propuesta alcanzará sus objetivos específicos de manera efectiva. La Comisión se encargará de hacer un seguimiento de los efectos de la propuesta. A tal fin, establecerá un sistema destinado a registrar aplicaciones de IA de alto riesgo independientes en una base de datos pública para toda la UE. Este registro también permitirá que las autoridades competentes, los usuarios y otras personas interesadas verifiquen si un sistema de IA de alto riesgo cumple los requisitos estipulados en la propuesta y ejerzan una vigilancia reforzada de aquellos sistemas de IA que entrañan un alto riesgo para los derechos fundamentales. Para alimentar esta base de datos, los proveedores de IA estarán obligados a facilitar información significativa sobre sus sistemas y la evaluación de la conformidad a la que los sometan.

Asimismo, los proveedores de IA tendrán la obligación de informar a las autoridades nacionales competentes de los incidentes graves o defectos de funcionamiento que constituyan un incumplimiento de sus obligaciones respecto de los derechos fundamentales en cuanto tengan constancia de ellos, así como de cualquier recuperación o retirada de sistemas de IA del mercado. A continuación, las autoridades nacionales competentes investigarán los incidentes o defectos de funcionamiento, recabarán toda la información necesaria y se la transmitirán periódicamente a la Comisión junto con los metadatos correspondientes. La Comisión complementará esta información sobre los incidentes con un análisis integral del mercado general de la IA.

La Comisión publicará un informe que evalúe y revise el marco de IA propuesto cinco años después de la fecha de entrada en vigor de dicho marco.

5.2. Explicación detallada de las disposiciones específicas de la propuesta

5.2.1. ÁMBITO DE APLICACIÓN Y DEFINICIONES (TÍTULO I)

En el **título I** se define el objeto del Reglamento y el ámbito de aplicación de las nuevas normas que abarcan la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA. Además, se establecen las definiciones utilizadas en todo el instrumento. La definición de «sistema de IA» que figura en el marco jurídico pretende ser lo más tecnológicamente neutra posible y resistir al paso del tiempo lo mejor posible, habida cuenta de la rápida evolución tecnológica y del mercado en relación con la IA. Con el objetivo de proporcionar la seguridad jurídica necesaria, el título I se complementa con el anexo I, que contiene una lista detallada de las estrategias y técnicas para el desarrollo de la IA que la Comisión deberá adaptar a los nuevos avances tecnológicos. También se proporciona una definición clara de los principales participantes en la cadena de valor de la IA, como los proveedores y los usuarios de sistemas de IA, entre los que se incluyen los operadores públicos y privados para garantizar la igualdad de condiciones.

5.2.2. PRÁCTICAS DE INTELIGENCIA ARTIFICIAL PROHIBIDAS (TÍTULO II)

En el **título II** se establece una lista de IA prohibidas. El Reglamento sigue un enfoque basado en los riesgos que distingue entre los usos de la IA que generan i) un riesgo inaceptable, ii) un riesgo alto, y iii) un riesgo bajo o mínimo. La lista de prácticas prohibidas que figura en el título II abarca todos los sistemas de IA cuyo uso se considera inaceptable por ser contrario a los valores de la Unión, por ejemplo, porque violan derechos fundamentales. Las prohibiciones engloban aquellas prácticas que tienen un gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es

probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas. La legislación vigente en materia de protección de datos, protección de los consumidores y servicios digitales, que garantiza que las personas físicas sean debidamente informadas y puedan decidir libremente no ser sometidas a la elaboración de perfiles u otras prácticas que puedan afectar a su conducta, podría cubrir otras prácticas de manipulación o de explotación contra adultos que los sistemas de IA pueden facilitar. La propuesta prohíbe igualmente que las autoridades públicas realicen calificación social basada en IA con fines generales. Por último, también se prohíbe, salvo excepciones limitadas, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley.

5.2.3. SISTEMAS DE ALTO RIESGO (TÍTULO III)

El **título III** contiene normas específicas para aquellos sistemas de IA que acarrean un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas. En consonancia con un enfoque basado en los riesgos, dichos sistemas de IA de alto riesgo están permitidos en el mercado europeo siempre que cumplan determinados requisitos obligatorios y sean sometidos a una evaluación de la conformidad *ex ante*. Un sistema de IA se considera de alto riesgo en función de su finalidad prevista, conforme a la legislación vigente relativa a la seguridad de los productos. Por lo tanto, la clasificación de un sistema de IA como de alto riesgo no depende únicamente de la función que lleve a cabo, sino también de la finalidad específica y de las modalidades para las que se use dicho sistema.

En el capítulo 1 del título III se establecen las normas de clasificación y se definen las dos categorías principales de sistemas de IA de alto riesgo:

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

La lista de sistemas de IA de alto riesgo que figura en el anexo III contiene un número limitado de sistemas de IA cuyos riesgos ya se han materializado o es probable que lo hagan próximamente. La Comisión podría ampliar la lista de sistemas de IA de alto riesgo utilizados en determinados ámbitos predefinidos mediante la aplicación de un conjunto de criterios y una metodología de evaluación del riesgo, a fin de garantizar que el Reglamento pueda adaptarse a los nuevos usos y aplicaciones de la IA.

En el capítulo 2 se establecen los requisitos legales que deben cumplir los sistemas de IA de alto riesgo en lo que respecta a los datos y su gobernanza, la documentación y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la seguridad. Muchos operadores diligentes que se encuentran a la vanguardia ya aplican los requisitos mínimos propuestos, que son el resultado de dos años de trabajos preparatorios y se derivan de las directrices éticas para una IA fiable elaboradas por el grupo de expertos de alto nivel sobre IA[29], ya aplicadas a modo de prueba por más de 350 organizaciones[30]. También son en gran medida coherentes con otras recomendaciones y principios internacionales, lo que garantiza la compatibilidad del marco propuesto para la IA

[29] Grupo de expertos de alto nivel sobre IA, *Directrices éticas para una IA fiable*, 2019.

[30] La Comisión también las respaldó en su Comunicación de 2019 relativa a una IA centrada en el ser humano.

con los adoptados por los socios comerciales internacionales de la UE. Las soluciones técnicas exactas que se necesitarán para lograr el cumplimiento de tales requisitos podrían proceder de normas u otras especificaciones técnicas, o bien desarrollarse con arreglo a los conocimientos científicos o de ingeniería generales, a discreción del proveedor del sistema de IA de que se trate. Esta flexibilidad reviste una importancia especial, ya que permite a los proveedores de sistemas de IA decidir cómo quieren cumplir los requisitos, teniendo en cuenta el estado de la técnica y los avances tecnológicos y científicos en este campo.

En el capítulo 3 se impone un conjunto claro de obligaciones horizontales a los proveedores de sistemas de IA de alto riesgo. También se establecen obligaciones proporcionadas para los usuarios y otros participantes de la cadena de valor de la IA (p. ej., los importadores, los distribuidores y los representantes autorizados).

En el capítulo 4 se establece el marco para que los organismos notificados participen en los procedimientos de evaluación de la conformidad como terceros independientes, mientras que en el capítulo 5 se explican en detalle los procedimientos de evaluación de la conformidad que deben seguirse para cada tipo de sistema de IA de alto riesgo. Con la evaluación de la conformidad se busca reducir al mínimo la carga que deben soportar los operadores económicos y los organismos notificados, cuya capacidad tiene que aumentar progresivamente con el tiempo. Los sistemas de IA destinados a ser utilizados como componentes de seguridad de productos regulados por la legislación del nuevo marco legislativo (p. ej., máquinas, productos sanitarios o juguetes) estarán sujetos a los mismos mecanismos de cumplimiento y aplicación *ex ante* y *ex post* que los productos de los que forman parte. La principal diferencia es que dichos mecanismos *ex ante* y *ex post* garantizarán el cumplimiento tanto de los requisitos establecidos en la legislación sectorial como de los previstos en este Reglamento.

Por otro lado, se establecerá un nuevo sistema de cumplimiento y aplicación para los sistemas de IA de alto riesgo independientes que se mencionan en el anexo III. Este seguirá el modelo de la legislación del nuevo marco legislativo que los proveedores aplicarán mediante controles internos, con la salvedad de los sistemas de identificación biométrica remota, que se someterán a evaluaciones de la conformidad efectuadas por terceros. Una solución efectiva y razonable para dichos sistemas podría consistir en realizar una evaluación integral de la conformidad *ex ante* mediante controles internos, combinada con una supervisión *ex post* estricta, dado que la intervención reguladora se encuentra en una fase temprana, que el sector de la IA es muy innovador y que apenas están empezando a acumularse los conocimientos necesarios para llevar a cabo auditorías. Para evaluar los sistemas de IA de alto riesgo «independientes» mediante controles internos, sería necesario cumplir *ex ante* de manera plena, efectiva y debidamente documentada todos los requisitos del Reglamento, así como los sólidos sistemas de gestión de la calidad y los riesgos y el seguimiento posterior a la comercialización. Una vez que el proveedor haya llevado a cabo la evaluación de la conformidad oportuna, deberá registrar dichos sistemas de IA de alto riesgo independientes en una base de datos de la UE que la Comisión gestionará con el propósito de redoblar la transparencia y la vigilancia públicas y de fortalecer la supervisión *ex post* por parte de las autoridades competentes. En cambio, por motivos de coherencia con la legislación vigente relativa a la seguridad de los productos, la evaluación de la conformidad de los sistemas de IA que son componentes de seguridad de productos seguirá un sistema en el que terceros llevarán a cabo procedimientos de evaluación de la conformidad ya definidos en la legislación sectorial sobre seguridad de los productos pertinente. Si se realizan modificaciones sustanciales en los sistemas de IA (fundamentalmente cambios que trasciendan los aspectos predeterminados por el proveedor en su documentación técnica y que se hayan comprobado

en la evaluación de la conformidad *ex ante*), habrá que realizar nuevas evaluaciones de la conformidad *ex ante*.

5.2.4. OBLIGACIONES DE TRANSPARENCIA PARA DETERMINADOS SISTEMAS DE IA (TÍTULO IV)

El **título IV** se centra en determinados sistemas de IA para tener en cuenta los riesgos específicos de manipulación que conllevan. Se aplicarán obligaciones de transparencia a los sistemas que i) interactúen con seres humanos, ii) se utilicen para detectar emociones o determinar la asociación a categorías (sociales) concretas a partir de datos biométricos, o iii) generen o manipulen contenido (ultrafalsificaciones). Cuando una persona interactúe con un sistema de IA o sus emociones o características sean reconocidas por medios automatizados, es preciso informarla de tal circunstancia. Si un sistema de IA se utiliza para generar o manipular imágenes, audios o vídeos que a simple vista parezcan contenido auténtico, debe ser obligatorio informar de que dicho contenido se ha generado por medios automatizados, salvo excepciones que respondan a fines legítimos (aplicación de la ley, libertad de expresión). De este modo, las personas pueden adoptar decisiones fundamentadas o evitar una situación determinada.

5.2.5. MEDIDAS EN FAVOR DE LA INNOVACIÓN (TÍTULO V)

El **título V** contribuye al objetivo de crear un marco jurídico que favorezca la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones. A tal fin, anima a las autoridades nacionales competentes a crear espacios controlados de pruebas y establece un marco básico en términos de gobernanza, supervisión y responsabilidad. Los espacios controlados de pruebas para la IA generan un entorno controlado para probar, durante un tiempo limitado, tecnologías innovadoras sobre la base de un plan de pruebas acordado con las autoridades competentes. El título V también contiene medidas encaminadas a reducir la carga normativa que deben soportar las pymes y las empresas emergentes.

5.2.6. GOBERNANZA Y APLICACIÓN (TÍTULOS VI, VII Y VIII)

En el **título VI** se establecen los sistemas de gobernanza nacionales y a escala de la Unión. En la Unión, la propuesta establece un Comité Europeo de Inteligencia Artificial («el Comité»), integrado por representantes de los Estados miembros y la Comisión. El Comité facilitará la aplicación sencilla, efectiva y armonizada de este Reglamento contribuyendo a la cooperación efectiva de las autoridades nacionales de supervisión y la Comisión, así como proporcionando asesoramiento y conocimientos especializados a esta última. Además, compilará y compartirá las mejores prácticas entre los Estados miembros.

En el plano nacional, los Estados miembros tendrán que designar a una o más autoridades nacionales competentes y, entre ellas, seleccionar a una autoridad nacional de supervisión que se encargará de supervisar la aplicación y ejecución del Reglamento. El Supervisor Europeo de Protección de Datos actuará como la autoridad competente para la supervisión de las instituciones, las agencias y los organismos de la Unión cuando entren en el ámbito de aplicación del presente Reglamento.

El **título VII** tiene por objeto facilitar la labor de seguimiento de la Comisión y las autoridades nacionales mediante el establecimiento de una base de datos para toda la UE donde figuren los sistemas de IA de alto riesgo independientes con implicaciones principalmente para los derechos fundamentales. Dicha base de datos, que gestionará la Comisión, contendrá los datos que faciliten los proveedores de sistemas de IA, los cuales estarán obligados a registrar sus sistemas antes de introducirlos en el mercado o ponerlos en servicio.

En el **título VIII** se definen las obligaciones de seguimiento y presentación de información que deben cumplir los proveedores de sistemas de IA en relación con el seguimiento posterior a la comercialización y la comunicación e investigación de incidentes y defectos de funcionamiento relacionados con la IA. Las autoridades de vigilancia del mercado controlarían también el mercado e investigarían el cumplimiento de las obligaciones y los requisitos aplicables a todos los sistemas de IA de alto riesgo que ya se han introducido en el mercado. Las autoridades de vigilancia del mercado tendrían todas las competencias previstas en el Reglamento (UE) 2019/1020 relativo a la vigilancia del mercado. La supervisión *ex post* debe garantizar que, una vez que un sistema de IA esté en el mercado, las autoridades públicas tengan las competencias y los recursos necesarios para intervenir en caso de que este genere riesgos inesperados, lo que justificaría una rápida actuación. Asimismo, también vigilarán que los operadores cumplan las obligaciones oportunas que les imponga el Reglamento. La propuesta no contempla la creación automática de organismos o autoridades adicionales en los Estados miembros. En consecuencia, los Estados miembros podrían designar a las autoridades sectoriales existentes, a las que también confiarían las competencias para vigilar y aplicar las disposiciones del Reglamento, aprovechando así sus conocimientos especializados.

Todo lo anterior debe interpretarse sin perjuicio del sistema y el reparto de competencias existentes para la supervisión *ex post* de las obligaciones relacionadas con los derechos fundamentales en los Estados miembros. Cuando sea necesario para el cumplimiento de sus respectivos mandatos, las autoridades de vigilancia y supervisión existentes también estarán facultadas para solicitar cualquier documentación que se conserve en virtud de este Reglamento, acceder a ella y, cuando proceda, pedir a las autoridades de vigilancia del mercado que organicen pruebas del sistema de IA de alto riesgo de que se trate por medios técnicos.

5.2.7. CÓDIGOS DE CONDUCTA (TÍTULO IX)

El **título IX** crea un marco para la elaboración de códigos de conducta, cuyo objetivo es fomentar que los proveedores de sistemas de IA que no son de alto riesgo cumplan de manera voluntaria los requisitos que son obligatorios para los sistemas de IA de alto riesgo (que se definen en el título III). Los proveedores de sistemas de IA que no son de alto riesgo podrían crear y aplicar sus propios códigos de conducta. Estos códigos también podrían incluir compromisos voluntarios relativos, por ejemplo, a la sostenibilidad medioambiental, la accesibilidad para las personas con discapacidad, la participación de las partes interesadas en el diseño y el desarrollo de sistemas de IA, y la diversidad de los equipos de desarrollo.

5.2.8. DISPOSICIONES FINALES (TÍTULOS X, XI Y XII)

El **título X** hace hincapié en la obligación de todas las partes de respetar la confidencialidad de la información y los datos, y establece normas para el intercambio de la información que se obtenga durante la aplicación del Reglamento. Asimismo, contiene medidas para garantizar la aplicación efectiva del Reglamento mediante la ejecución de sanciones efectivas, proporcionadas y disuasorias en caso de que se incumplan sus disposiciones.

En el **título XI** se establecen las normas para el ejercicio de las competencias de delegación y de ejecución. La propuesta faculta a la Comisión para adoptar, cuando corresponda, actos de ejecución que garanticen la aplicación uniforme del Reglamento o actos delegados destinados a actualizar o complementar las listas que figuran en los anexos I a VII.

En el **título XII** se recoge la obligación de la Comisión de evaluar regularmente la necesidad de actualizar el anexo III y preparar informes periódicos sobre la evaluación y el examen del Reglamento. Asimismo, establece las disposiciones finales, entre ellas un período transitorio

diferenciado para la fecha inicial de aplicabilidad del Reglamento, a fin de facilitar una aplicación fluida para todas las partes implicadas.

2021/0106 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE 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,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[31],

Visto el dictamen del Comité de las Regiones[32],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interno mediante el establecimiento de un marco jurídico uniforme, en particular en lo que respecta al desarrollo, la comercialización y la utilización de la inteligencia artificial de conformidad con los valores de la Unión. El presente Reglamento persigue varios fines imperiosos de interés general, tales como asegurar un nivel elevado de protección de la salud, la seguridad y los derechos humanos, y garantiza la libre circulación transfronteriza de bienes y servicios basados en la IA, con lo que impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente.

(2) Los sistemas de inteligencia artificial («sistemas de IA») pueden emplearse con facilidad en múltiples sectores de la economía y la sociedad, también a escala transfronteriza, y circular por toda la Unión. Algunos Estados miembros ya han estudiado la posibilidad de adoptar normas nacionales destinadas a garantizar que la inteligencia artificial sea segura y se desarrolle y utilice de conformidad con las obligaciones relativas a los derechos fundamentales. La existencia de distintas normas nacionales puede dar lugar a la fragmentación del mercado interior y reducir la seguridad jurídica de los operadores que desarrollan o utilizan sistemas de IA. Por lo tanto, es preciso garantizar un nivel elevado y coherente de protección en toda la Unión y evitar las divergencias que obstaculizan la libre circulación en el mercado interior de los sistemas de IA y los productos y servicios conexos mediante el establecimiento de obligaciones uniformes para todos los operadores y la garantía de

[31] DO C […] de […], p. […].
[32] DO C […] de […], p. […].

una protección uniforme de los fines imperiosos de interés general 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 para la protección de las personas en relación con el tratamiento de datos personales que restringen el uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, resulta adecuado basar este Reglamento, en lo que atañe a dichas normas específicas, en el artículo 16 del TFUE. A la luz de dichas normas específicas y de la invocación del artículo 16 del TFUE, conviene consultar al Comité Europeo de Protección de Datos.

(3) La inteligencia artificial es un conjunto de tecnologías de rápida evolución que puede generar un amplio abanico de beneficios económicos y sociales en todos los sectores y actividades sociales. El uso de la inteligencia artificial puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de la asistencia sanitaria, la agricultura, la educación y la formación, la administración de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, y la mitigación del cambio climático y la adaptación a él, entre otros, al mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones.

(4) Al mismo tiempo, dependiendo de las circunstancias de su aplicación y utilización concretas, la inteligencia artificial puede generar riesgos y menoscabar los intereses públicos y los derechos que protege el Derecho de la Unión, de manera tangible o intangible.

(5) Por este motivo, se necesita un marco jurídico de la Unión que defina unas normas armonizadas en materia de inteligencia artificial orientadas a impulsar el desarrollo, la utilización y la adopción en el mercado interior de la inteligencia artificial y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad, y de los derechos fundamentales reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado y la puesta en servicio de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de la libre circulación de bienes y servicios. Al establecer tales normas, el presente Reglamento respalda el objetivo de la Unión de ser un líder mundial en el desarrollo de inteligencia artificial segura, digna de confianza y ética, como indicó el Consejo Europeo[33], y garantiza la protección de los principios éticos, como solicitó específicamente el Parlamento Europeo[34].

(6) Resulta necesario definir con claridad la noción de sistema de IA para ofrecer seguridad jurídica, al mismo tiempo que se proporciona la flexibilidad necesaria para adaptarse a los futuros avances tecnológicos. La definición debe basarse en las principales características funcionales del *software*, y en particular en su capacidad para generar, en relación con un conjunto concreto de objetivos definidos por seres

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

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

humanos, contenidos, predicciones, recomendaciones, decisiones u otra información de salida que influyan en el entorno con el que interactúa el sistema, ya sea en una dimensión física o digital. Los sistemas de IA pueden diseñarse para operar con distintos niveles de autonomía y utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente de él (integrado) o tiene una funcionalidad en el producto sin formar parte de él (no integrado). La definición de «sistema de IA» debe complementarse con una lista de las técnicas y estrategias concretas que se usan en su desarrollo. Dicha lista debe estar actualizada atendiendo a los avances tecnológicos y del mercado, para lo cual la Comisión debe adoptar actos delegados que la modifiquen.

(7) La noción de «datos biométricos» empleada en el presente Reglamento coincide con la noción de «datos biométricos» definida en el artículo 4, punto 14, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[35]; en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[36]; y en el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[37], y debe interpretarse en consonancia con ella.

(8) La noción de «sistema de identificación biométrica remota» que se utiliza en este Reglamento debe definirse de manera funcional, como un sistema de IA destinado a identificar a distancia a personas físicas comparando sus datos biométricos con los que figuren en una base de datos de referencia, sin saber de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen. Es preciso distinguir entre los sistemas de identificación biométrica remota «en tiempo real» y «en diferido», dado que tienen características distintas, se utilizan de manera diferente y entrañan riesgos distintos. En el caso de los sistemas «en tiempo real», la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, casi instantánea o, en cualquier caso, sin una demora significativa. En este sentido, no debe existir la posibilidad de eludir las normas contempladas en el presente Reglamento en relación con el uso «en tiempo real» de los sistemas de IA en cuestión generando demoras mínimas. Los sistemas «en tiempo real» implican el uso de material «en directo» o «casi en directo», como grabaciones de vídeo generadas por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas «en diferido» los datos ya se han recabado y la comparación e identificación se producen con una demora significativa. A tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de

---

35 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).

36 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 esos 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).

37 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva sobre protección de datos en el ámbito penal) (DO L 119 de 4.5.2016, p. 89).

televisión en circuito cerrado o dispositivos privados, que se han generado antes de aplicar el sistema a las personas físicas en cuestión.

(9) A los efectos del presente Reglamento, se entenderá que «espacio de acceso público» se refiere a cualquier lugar físico al que tenga acceso el público, con independencia de si es de propiedad privada o pública. Por consiguiente, esta noción no abarca aquellos lugares de carácter privado a los que, por lo general, no pueden acceder libremente terceros, incluidas las fuerzas o cuerpos de seguridad, a menos que hayan sido invitados o autorizados específicamente, como viviendas, clubes privados, oficinas, almacenes y fábricas. Tampoco cubre los espacios en línea, ya que no son espacios físicos. No obstante, el simple hecho de que deban cumplirse determinadas condiciones para acceder a un espacio concreto, como la adquisición de entradas o las restricciones en relación con la edad, no significa que este no sea de acceso público en el sentido del presente Reglamento. En consecuencia, además de espacios públicos como las calles, las zonas pertinentes de edificios gubernamentales y la mayoría de las infraestructuras de transporte, normalmente también se consideran de acceso público espacios como cines, teatros, tiendas y centros comerciales. No obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta.

(10) Con el objetivo de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas en el presente Reglamento deben aplicarse a los proveedores de sistemas de IA sin discriminación, con independencia de si están establecidos en la Unión o en un tercer país, y a los usuarios de sistemas de IA establecidos en la Unión.

(11) Debido a su carácter digital, algunos sistemas de IA deben entrar en el ámbito de aplicación del presente Reglamento aunque no se introduzcan en el mercado, se pongan en servicio ni se utilicen en la Unión. Tal es el caso, por ejemplo, de un operador establecido en la Unión que contrate determinados servicios a otro operador establecido fuera de la Unión en relación con una actividad que llevará a cabo un sistema de IA que se consideraría de alto riesgo y que tiene repercusiones para las personas físicas ubicadas en la Unión. En dichas circunstancias, el sistema de IA usado por el operador de fuera de la Unión podría tratar datos recabados legalmente en la UE y transferidos desde su territorio, y proporcionar al operador contratante ubicado en la Unión la información de salida generada por dicho sistema de IA a raíz de su tratamiento, sin que el sistema de IA en cuestión se introduzca en el mercado, se ponga en servicio o se utilice en la Unión. Para evitar la elusión de este Reglamento y asegurar la protección efectiva de las personas físicas ubicadas en la Unión, el presente Reglamento también debe aplicarse a los proveedores y usuarios de sistemas de IA establecidos en un tercer país, en la medida en que la información de salida generada por dichos sistemas se utilice en la Unión. No obstante, con el objetivo de tener en cuenta los acuerdos existentes y las necesidades especiales de cooperación con socios extranjeros con los que se intercambian información y pruebas, el presente Reglamento no debe aplicarse a las autoridades públicas de un tercer país ni a las organizaciones internacionales cuando actúen en el marco de acuerdos internacionales celebrados a escala nacional o europea con fines de cooperación policial y judicial con la Unión o sus Estados miembros. Dichos acuerdos se han celebrado 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.

(12) El presente Reglamento debe aplicarse igualmente a las instituciones, las oficinas, los organismos y las agencias de la Unión cuando actúen como proveedores o usuarios de

un sistema de IA. Los sistemas de IA desarrollados o utilizados exclusivamente con fines militares deben quedar excluidos del ámbito de aplicación del presente Reglamento cuando su uso sea competencia exclusiva de la política exterior y de seguridad común regulada en el título V del Tratado de la Unión Europea (TUE). El presente Reglamento debe interpretarse sin perjuicio de las disposiciones de la Directiva 2000/31/CE del Parlamento Europeo y el Consejo (en su versión modificada por la Ley de Servicios Digitales) relativas a la responsabilidad de los prestadores de servicios intermediarios.

(13) Conviene establecer normas comunes para todos los sistemas de IA de alto riesgo al objeto de garantizar un nivel elevado y coherente de protección de los intereses públicos en lo que respecta a la salud, la seguridad y los derechos fundamentales. Dichas normas deben ser coherentes con la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»), no deben ser discriminatorias y deben estar en consonancia con los compromisos de la Unión en materia de comercio internacional.

(14) Con el fin de introducir un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, es preciso aplicar un enfoque basado en los riesgos claramente definido, que adapte el tipo de las normas y su contenido a la intensidad y el alcance de los riesgos que puedan generar los sistemas de IA en cuestión. Por consiguiente, es necesario prohibir determinadas prácticas de inteligencia artificial, definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, e imponer obligaciones de transparencia a determinados sistemas de IA.

(15) Al margen de los múltiples usos beneficiosos de la inteligencia artificial, dicha tecnología también puede utilizarse indebidamente y proporcionar nuevas y poderosas herramientas para llevar a cabo prácticas de manipulación, explotación y control social. Dichas prácticas son sumamente perjudiciales y deben estar prohibidas, pues van en contra de los valores de la Unión de respeto de la dignidad humana, libertad, igualdad, democracia y Estado de Derecho y de los derechos fundamentales que reconoce la UE, como el derecho a la no discriminación, la protección de datos y la privacidad, y los derechos del niño.

(16) Debe prohibirse la introducción en el mercado, la puesta en servicio o el uso de determinados sistemas de IA destinados a alterar la conducta humana que es probable que provoquen perjuicios físicos o psicológicos. Dichos sistemas de IA despliegan componentes subliminales imperceptibles para el ser humano o se aprovechan de las vulnerabilidades de los menores y las personas por razones de edad o incapacidad física o mental. Lo hacen con la intención de alterar sustancialmente el comportamiento de una persona y de un modo que perjudique o es probable que perjudique a esa misma persona o a otra. Dicha intención no puede darse por supuesta si la alteración del comportamiento humano es el resultado de factores externos al sistema de IA que escapan al control del proveedor o el usuario. Su prohibición no debe impedir la investigación relacionada con esos sistemas de IA con fines legítimos, siempre que tal investigación no implique usar el sistema de IA en cuestión en relaciones entre seres humanos y máquinas que expongan a personas físicas a perjuicios, y siempre que se lleve a cabo con arreglo a las normas éticas reconocidas para la investigación científica.

(17) Los sistemas de IA que proporcionan calificaciones sociales de personas físicas para su uso con fines generales por parte de las autoridades públicas o en representación de estas pueden tener resultados discriminatorios y abocar a la exclusión a determinados

grupos. Pueden menoscabar el derecho a la dignidad y la no discriminación y los valores de igualdad y justicia. Dichos sistemas de IA evalúan o clasifican la fiabilidad de las personas físicas en función de su comportamiento social en múltiples contextos o de características personales o de su personalidad conocidas o predichas. La calificación social resultante de dichos sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de personas físicas o colectivos enteros en contextos sociales que no guardan relación con el contexto donde se generaron o recabaron los datos originalmente, o a un trato perjudicial desproporcionado o injustificado en relación con la gravedad de su comportamiento social. Por lo tanto, dichos sistemas de IA deben prohibirse.

(18) Se considera que el uso de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley invade especialmente los derechos y las libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales. Además, la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales en relación con el uso de sistemas que operan «en tiempo real» acrecientan el riesgo para los derechos y las libertades de las personas afectadas por las actividades de aplicación de la ley.

(19) En consecuencia, debe prohibirse el uso de dichos sistemas con fines de aplicación de la ley, salvo en tres situaciones enumeradas de manera limitativa y definidas con precisión en las que su utilización es estrictamente necesaria para lograr un interés público esencial cuya importancia es superior a los riesgos. Estas situaciones son la búsqueda de posibles víctimas de un delito, incluidos menores desaparecidos; determinadas amenazas para la vida o la seguridad física de las personas físicas o amenazas de atentado terrorista; y la detección, la localización, la identificación o el enjuiciamiento de los autores o sospechosos de los delitos mencionados en la Decisión Marco 2002/584/JAI del Consejo[38], si la normativa del Estado miembro implicado señala una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos de tres años, tal como se definan en el Derecho de dicho Estado miembro. Fijar ese umbral para la pena o la medida de seguridad privativas de libertad con arreglo al Derecho nacional contribuye a garantizar que el delito sea lo suficientemente grave como para llegar a justificar el uso de sistemas de identificación biométrica remota «en tiempo real». Por otro lado, en la práctica, algunos de los treinta y dos delitos enumerados en la Decisión Marco 2002/584/JAI del Consejo son probablemente más relevantes que otros en el sentido de que, previsiblemente, recurrir a la identificación biométrica remota «en tiempo real» se considerará necesario y proporcionado en grados muy distintos para llevar a cabo la detección, la localización, la identificación o el enjuiciamiento de los autores o sospechosos de tales delitos, como también habrá enormes diferencias en la gravedad, la probabilidad y la magnitud de los perjuicios o las posibles consecuencias negativas que se deriven de ellos.

(20) Para velar por que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en esas tres situaciones enumeradas de manera limitativa y definidas con precisión, deben tenerse en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que dé lugar a la

[38] 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).

solicitud, a las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas, y a las salvaguardias y condiciones que acompañen a su uso. Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar sujeto a límites temporales y espaciales adecuados que tengan en cuenta, en particular, las pruebas o indicios relativos a las amenazas, las víctimas o los autores. La base de datos de personas de referencia debe ser adecuada para cada caso de uso en cada una de las tres situaciones antes mencionadas.

(21) Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro. En principio, dicha autorización debe obtenerse con anterioridad al uso, excepto en situaciones de urgencia debidamente justificadas, es decir, aquellas en las que la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso. En tales situaciones de urgencia, el uso debe limitarse al mínimo imprescindible y cumplir las salvaguardias y las condiciones oportunas, conforme a lo estipulado en el Derecho interno y según corresponda en cada caso concreto de uso urgente por parte de las fuerzas o cuerpos de seguridad. Además, en esas situaciones las fuerzas o cuerpos de seguridad deben tratar de obtener una autorización lo antes posible e indicar los motivos por los que no han podido hacerlo antes.

(22) Por otro lado, conviene estipular, en el marco exhaustivo que establece este Reglamento, que dicho uso en el territorio de un Estado miembro conforme a lo dispuesto en el presente Reglamento solo debe ser posible cuando el Estado miembro en cuestión haya decidido contemplar expresamente la posibilidad de autorizarlo en las normas detalladas de su Derecho interno, y en la medida en que lo haya contemplado. En consecuencia, con el presente Reglamento los Estados miembros siguen siendo libres de no ofrecer esta posibilidad en absoluto o de ofrecerla únicamente en relación con algunos de los objetivos que pueden justificar un uso autorizado conforme al presente Reglamento.

(23) La utilización de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley implica, necesariamente, el tratamiento de datos biométricos. Las normas del presente Reglamento que prohíben, con algunas excepciones, ese uso, basadas en el artículo 16 del TFUE, deben aplicarse como *lex specialis* con respecto a las normas sobre el tratamiento de datos biométricos que figuran en el artículo 10 de la Directiva (UE) 2016/680, con lo que se regula de manera exhaustiva dicho uso y el tratamiento de los datos biométricos conexos. Por lo tanto, ese uso y tratamiento solo deben ser posibles en la medida en que sean compatibles con el marco establecido por el presente Reglamento, sin que exista un margen, fuera de dicho marco, para que las autoridades competentes, cuando actúen con fines de aplicación de la ley, utilicen tales sistemas y traten los datos conexos en los supuestos previstos en el artículo 10 de la Directiva (UE) 2016/680. En este contexto, el presente Reglamento no pretende sentar la base jurídica para el tratamiento de datos personales en virtud del artículo 8 de la Directiva (UE) 2016/680. Sin embargo, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines distintos de la aplicación de la ley, incluso por parte de las autoridades competentes, no debe estar cubierto por el marco específico establecido por el presente Reglamento en lo que

respecta al uso de dichos sistemas con fines de aplicación de la ley. Por consiguiente, su uso con fines distintos de la aplicación de la ley no debe supeditarse al requisito de obtener una autorización previsto en este Reglamento ni a las normas detalladas del Derecho interno aplicables que pudieran hacerlo efectivo.

(24) Todo tratamiento de datos biométricos y datos personales de otra índole asociado al uso de sistemas de IA con fines de identificación biométrica distinto del uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley regulado por el presente Reglamento debe seguir cumpliendo todos los requisitos derivados del artículo 9, apartado 1, del Reglamento (UE) 2016/679; el artículo 10, apartado 1, del Reglamento (UE) 2018/1725, y el artículo 10 de la Directiva (UE) 2016/680, según corresponda, incluso cuando las autoridades competentes sean quienes usen dichos sistemas en espacios de acceso público con fines distintos de la aplicación de la ley.

(25) De conformidad con el artículo 6 *bis* del Protocolo n.º 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 queda obligada por las normas establecidas en el artículo 5, apartado 1, letra d), y el artículo 5, apartados 2 y 3, del presente Reglamento, adoptadas sobre la base del artículo 16 del TFUE, que se refieren al tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 4 o el capítulo 5 del título V de la tercera parte del TFUE, en la medida en que no Irlanda no quede obligada por las normas que regulen formas de cooperación judicial en materia penal o de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas sobre la base del artículo 16 del TFUE.

(26) De conformidad con lo dispuesto en los artículos 2 y 2 *bis* del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no queda obligada las normas establecidas en el artículo 5, apartado 1, letra d), y el artículo 5, apartados 2 y 3, del presente Reglamento, adoptadas sobre la base del artículo 16 del TFUE, que se relacionen con el tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 4 o el capítulo 5 del título V de la tercera parte del TFUE, ni está sujeta a su aplicación.

(27) La introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo en la Unión debe supeditarse al cumplimiento por su parte de determinados requisitos obligatorios, los cuales deben garantizar que los sistemas de IA de alto riesgo disponibles en la Unión o cuya información de salida se utilice en la Unión no entrañen riesgos inaceptables para intereses públicos importantes de la UE, reconocidos y protegidos por el Derecho de la Unión. La calificación «de alto riesgo» debe limitarse a aquellos sistemas de IA que tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación reduce al mínimo cualquier posible restricción del comercio internacional, si la hubiera.

(28) Los sistemas de IA pueden tener efectos adversos para la salud y la seguridad de las personas, en particular cuando funcionan como componentes de 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 velar por que solo lleguen al mercado aquellos productos que sean seguros y conformes, es importante prevenir y reducir debidamente los riesgos de seguridad que pueda generar un

producto en su conjunto debido a sus componentes digitales, entre los que pueden figurar los sistemas de IA. Por ejemplo, los robots cada vez más autónomos que se utilizan en las fábricas o con fines de asistencia y cuidado personal deben poder funcionar y desempeñar sus funciones de manera segura en entornos complejos. Del mismo modo, en el sector sanitario, donde los riesgos para la vida y la salud son especialmente elevados, los sistemas de diagnóstico y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, deben ser fiables y precisos. La magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es particularmente pertinente cuando este es clasificado como de alto riesgo. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, la no discriminación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración. Además de esos derechos, conviene poner de relieve que los menores poseen unos derechos específicos consagrados en el artículo 24 de la Carta de la UE y en la Convención sobre los Derechos del Niño de las Naciones Unidas, que se desarrollan en mayor profundidad en la observación general n.º 25 del Comité de los Derechos del Niño relativa a los derechos de los niños en relación con el entorno digital. Ambos instrumentos exigen que se tengan en consideración las vulnerabilidades de los menores y que se les brinde la protección y la asistencia necesarias para su bienestar. Cuando se evalúe la gravedad del perjuicio que puede ocasionar un sistema de IA, en particular en lo que respecta a la salud y la seguridad de las personas, también se debe tener en cuenta el derecho fundamental a un nivel elevado de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión.

(29) En cuanto 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 que entran en el ámbito de aplicación del Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo[39], el Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo[40], el Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo[41], la Directiva 2014/90/UE del Parlamento Europeo y del Consejo[42], la Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo[43], el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo[44], el Reglamento

[39] Reglamento (CE) n.º 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) n.º 2320/2002 (DO L 97 de 9.4.2008, p. 72).

[40] Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 1).

[41] Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, relativo a la homologación de los vehículos de dos o tres ruedas y los cuatriciclos, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 52).

[42] 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).

[43] 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).

[44] 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 sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se

(UE) 2018/1139 del Parlamento Europeo y del Consejo[45], y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo[46], procede modificar dichos actos para garantizar que, cuando la Comisión adopte en el futuro adopte actos delegados o de ejecución pertinentes en la materia basándose en ellos, tenga en cuenta los requisitos obligatorios para los sistemas de IA de alto riesgo previstos en el presente Reglamento, atendiendo a las particularidades técnicas y reglamentarias de los distintos sectores y sin interferir con la gobernanza, los mecanismos de evaluación de la conformidad y supervisión, y las autoridades existentes en cada uno de ellos.

(30) En cuanto a los sistemas de IA que son componentes de seguridad de productos, o que son productos en sí mismos, y entran dentro del ámbito de aplicación de determinada legislación de armonización de la Unión, procede considerarlos de alto riesgo en virtud del presente Reglamento si el producto en cuestión es sometido al procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad externo de acuerdo con dicha legislación de armonización pertinente de la Unión. Esos productos son, en concreto, máquinas, juguetes, ascensores, equipo y sistemas de protección para uso en atmósferas potencialmente explosivas, equipos radioeléctricos, equipos a presión, equipo de embarcaciones de recreo, instalaciones de transporte por cable, aparatos que queman combustibles gaseosos, productos sanitarios y productos sanitarios para diagnóstico *in vitro*.

(31) Que un sistema de IA se considere de alto riesgo en virtud del presente Reglamento no significa necesariamente que el producto del que sea componente de seguridad, o el sistema de IA en sí mismo como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto. Tal es el caso, en particular, del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo[47] y del Reglamento (UE) 2017/746 del Parlamento

---

modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y por el que se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1).

45 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 la Unión Europea para la Seguridad Aérea y por el que 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 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).

46 Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de 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) n.º 79/2009 y (CE) n.º 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (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 de la Comisión (DO L 325 de 16.12.2019, p. 1).

47 Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los 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 por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

Europeo y del Consejo[48], que prevén que un organismo independiente realice una evaluación de la conformidad de los productos de riesgo medio y alto.

(32) En cuanto a los sistemas de IA independientes, es decir, aquellos sistemas de IA de alto riesgo que no son componentes de seguridad de productos o no son productos en sí mismos, hay que considerarlos de alto riesgo si, a la luz de su finalidad prevista, presentan un alto riesgo de menoscabar la salud y la seguridad o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que se produzca, y se utilizan en varias esferas predefinidas especificadas en el presente Reglamento. Para identificar dichos sistemas se emplean la misma metodología y los mismos criterios previstos para la posible modificación futura de la lista de sistemas de IA de alto riesgo.

(33) Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y tener consecuencias discriminatorias. Esto es especialmente importante en lo que respecta a la edad, la etnia, el sexo o la discapacidad. Por este motivo, debe considerarse que los sistemas de identificación biométrica remota «en tiempo real» y «en diferido» conllevan un alto riesgo. Debido a los riesgos que entrañan, deben aplicarse requisitos específicos referentes a las capacidades de registro y la vigilancia humana a ambos tipos de sistemas de identificación biométrica remota.

(34) En el caso de la gestión y el funcionamiento de infraestructuras críticas, conviene considerar de alto riesgo a los sistemas de IA destinados a ser componentes de seguridad en la gestión y el funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad, pues su fallo o defecto de funcionamiento puede poner en peligro la vida y la salud de las personas a gran escala y alterar de manera apreciable el desarrollo habitual de las actividades sociales y económicas.

(35) Deben considerarse de alto riesgo los sistemas de IA que se utilizan en la educación o la formación profesional, y en especial aquellos que determinan el acceso o distribuyen a las personas entre distintas instituciones educativas y de formación profesional o aquellos que evalúan a las personas a partir de pruebas realizadas en el marco de su educación o como condición necesaria para acceder a ella, ya que pueden decidir la trayectoria formativa y profesional de una persona y, en consecuencia, afectar a su capacidad para asegurar su subsistencia. Cuando no se diseñan y utilizan correctamente, estos sistemas pueden violar el derecho a la educación y la formación, y el derecho a no sufrir discriminación, además de perpetuar patrones históricos de discriminación.

(36) También deben considerarse de alto riesgo los sistemas de IA que se utilizan en el empleo, la gestión de los trabajadores y el acceso al autoempleo, sobre todo para la contratación y la selección de personal; para la toma de decisiones relativas a la promoción y la rescisión de contratos; y para la asignación de tareas y el seguimiento o la evaluación de personas en relaciones contractuales de índole laboral, dado que pueden afectar de un modo considerable a las futuras perspectivas laborales y los medios de subsistencia de dichas personas. Las relaciones contractuales de índole laboral deben implicar a los empleados y las personas que prestan servicios a través de plataformas, como indica el Programa de trabajo de la Comisión para 2021. En

[48] Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los 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).

principio, esas personas no deben ser consideradas usuarios en el sentido del presente Reglamento. Dichos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, ciertos grupos de edad, personas con discapacidad o personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, la promoción o la retención de personas en relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden afectar a sus derechos a la protección de los datos personales y a la privacidad.

(37) El acceso y el disfrute de determinados servicios y ayudas esenciales de carácter público y privado necesarios para que las personas participen en la sociedad o cuenten con unas condiciones de vida mejores es otro ámbito en el que conviene prestar especial atención a la utilización de sistemas de IA. En concreto, deben considerarse de alto riesgo los sistemas de IA usados para evaluar la calificación crediticia o solvencia de personas físicas, ya que deciden si dichas personas pueden acceder a recursos financieros o servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones. Los sistemas de IA usados con este fin pueden discriminar a personas o grupos y perpetuar patrones históricos de discriminación, por ejemplo, por motivos de origen racial o étnico, discapacidad, edad u orientación sexual, o generar nuevas formas de efectos discriminatorios. Habida cuenta del alcance sumamente limitado de su impacto y de las escasas alternativas disponibles en el mercado, conviene dejar exentos a los sistemas de IA destinados a evaluar la solvencia y la calificación crediticia cuando los pongan en servicio proveedores a pequeña escala para su propio uso. Las personas físicas que solicitan o reciben ayudas y servicios de autoridades públicas suelen depender de ellos y, por lo general, se encuentran en una posición de vulnerabilidad respecto de las autoridades responsables. Si se utilizan sistemas de IA para decidir si las autoridades deben denegar, reducir, revocar o reclamar dichas ayudas y servicios, estos sistemas pueden afectar de un modo considerable a los medios de subsistencia de las personas y podrían infringir sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a una tutela judicial efectiva. Por lo tanto, esos sistemas deben considerarse de alto riesgo. No obstante, el presente Reglamento no debe obstaculizar el desarrollo y el uso de enfoques innovadores en la Administración pública, que se beneficiarían de una mayor utilización de sistemas de IA conformes y seguros, siempre y cuando dichos sistemas no conlleven un alto riesgo para las personas jurídicas y físicas. Por último, los sistemas de IA empleados para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia también deben considerarse de alto riesgo, dado que adoptan decisiones en situaciones sumamente críticas para la vida y la salud de las personas y de sus bienes.

(38) Las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta. En particular, si el sistema de IA no está entrenado con datos de buena calidad, no cumple los requisitos oportunos en términos de precisión o solidez, o no se diseña y prueba debidamente antes de introducirlo en el mercado o ponerlo en servicio, puede señalar a personas de manera discriminatoria, incorrecta o injusta. Además, podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez

imparcial, así como los derechos de la defensa y la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén bien documentados. Por consiguiente, procede considerar de alto riesgo a múltiples sistemas de IA diseñados para usarse con fines de aplicación de la ley cuando su precisión, fiabilidad y transparencia sean especialmente importantes para evitar consecuencias adversas, conservar la confianza de la población y garantizar la rendición de cuentas y una compensación efectiva. En vista de la naturaleza de las actividades en cuestión y de los riesgos conexos, entre dichos sistemas de IA de alto riesgo deben incluirse, en particular, los sistemas de IA que las autoridades encargadas de la aplicación de la ley utilicen para realizar evaluaciones del riesgo individuales, los polígrafos y herramientas similares, o los sistemas utilizados para detectar el estado emocional de una persona física; para detectar ultrafalsificaciones; para evaluar la fiabilidad de las pruebas en un proceso penal; para predecir la comisión o reiteración de un delito real o potencial mediante la elaboración de perfiles de personas físicas; para evaluar rasgos y características de la personalidad o conductas delictivas pasadas de personas físicas o grupos; para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de infracciones penales, y para realizar análisis penales en relación con personas físicas. No debe considerarse que los sistemas de IA destinados específicamente a que las autoridades fiscales y aduaneras los utilicen en procesos administrativos forman parte de los sistemas de IA de alto riesgo usados por las autoridades encargadas de la aplicación de la ley con el fin de prevenir, detectar, investigar y enjuiciar infracciones penales.

(39) Los sistemas de IA empleados en la gestión de la migración, el asilo y el control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilizan en estos contextos sean precisos, no discriminatorios y transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, sus derechos a la libre circulación, la no discriminación, la intimidad personal y la protección de los datos personales, la protección internacional y la buena administración. Por lo tanto, procede considerar de alto riesgo a aquellos sistemas de IA destinados a que las autoridades públicas competentes que realizan tareas en el ámbito de la gestión de la migración, el asilo y el control fronterizo los utilicen como polígrafos y herramientas similares o para detectar el estado emocional de una persona física; para evaluar determinados riesgos que presenten personas físicas que entren en el territorio de un Estado miembro o soliciten un visado o asilo; para verificar la autenticidad de los documentos pertinentes de personas físicas; para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado y permiso de residencia, así como las reclamaciones conexas en relación con el objetivo de determinar si las personas físicas solicitantes de un estatuto reúnen los requisitos necesarios para su obtención. Los sistemas de IA en el ámbito de la gestión de la migración, el asilo y el control fronterizo abarcados por el presente Reglamento deben cumplir los requisitos procedimentales pertinentes establecidos por la Directiva 2013/32/UE del Parlamento Europeo y del Consejo[49], el

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

Reglamento (UE) n.º 810/2009 del Parlamento Europeo y el Consejo[50], y otra legislación en la materia.

(40) Deben considerarse de alto riesgo ciertos sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de evitar el riesgo de posibles sesgos, errores y opacidades, procede considerar de alto riesgo aquellos sistemas de IA cuyo objetivo es ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. No obstante, dicha clasificación no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia en casos concretos, como la anonimización o seudonimización de las resoluciones judiciales, documentos o datos; la comunicación entre los miembros del personal; tareas administrativas, o la asignación de recursos.

(41) El hecho de que un sistema de IA sea considerado de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea legal con arreglo a otros actos del Derecho de la Unión o del Derecho interno compatible con el Derecho de la Unión relativo a la protección de los datos personales o a la utilización de polígrafos y herramientas similares u otros sistemas para detectar el estado emocional de las personas físicas. Todo uso de ese tipo debe seguir realizándose exclusivamente en consonancia con los requisitos oportunos derivados de la Carta y de los actos aplicables del Derecho derivado de la Unión y del Derecho interno. No debe entenderse que el presente Reglamento constituye el fundamento jurídico para el tratamiento de datos personales, incluidas categorías especiales de datos personales, cuando sea pertinente.

(42) Con el objetivo de mitigar los riesgos que presentan para los usuarios y las personas afectadas los sistemas de IA de alto riesgo que se introducen en el mercado o ponen en servicio en la Unión, es preciso aplicar ciertos requisitos obligatorios que tengan en cuenta la finalidad prevista del uso del sistema y estén en consonancia con el sistema de gestión de riesgos que debe establecer el proveedor.

(43) Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la calidad de los conjuntos de datos utilizados, la documentación técnica y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales, según corresponda en función de la finalidad prevista del sistema, y no se dispone razonablemente de otras medidas menos restrictivas del comercio, con lo que se evitan restricciones injustificadas de este.

(44) Muchos sistemas de IA necesitan datos de alta calidad para funcionar correctamente, en especial cuando se emplean técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funciona del modo previsto y en condiciones de seguridad y no se convierte en la fuente de alguno de los tipos de

[50] Reglamento (CE) n.º 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 de visados) (DO L 243 de 15.9.2009, p. 1).

discriminación prohibidos por el Derecho de la Unión. Es preciso instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos de entrenamiento, validación y prueba sean de buena calidad. Los conjuntos de datos de entrenamiento, validación y prueba deben ser lo suficientemente pertinentes y representativos, carecer de errores y ser completos en vista de la finalidad prevista del sistema. Asimismo, deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los grupos de personas en las que en un principio se usará el sistema de IA de alto riesgo. En concreto, los conjuntos de datos de entrenamiento, validación y prueba deben tener en cuenta, en la medida necesaria en función de su finalidad prevista, los rasgos, características o elementos particulares del entorno o contexto geográfico, conductual o funcional específico en el que se pretende utilizar el sistema de IA. Con el fin de proteger los derechos de terceros frente a la discriminación que podría provocar el sesgo de los sistemas de IA, los proveedores deben ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial, para garantizar que el sesgo de los sistemas de IA de alto riesgo se vigile, detecte y corrija.

(45) Para poder desarrollar sistemas de IA de alto riesgo, determinados agentes, tales como proveedores, organismos notificados y otras entidades pertinentes, como centros de innovación digital, centros de ensayo y experimentación e investigadores, deben tener acceso a conjuntos de datos de alta calidad en sus respectivos campos de actividad relacionados con el presente Reglamento y poder utilizarlos. Los espacios comunes europeos de datos establecidos por la Comisión y la facilitación del intercambio de datos entre empresas y con los Gobiernos en aras del interés público serán esenciales para brindar un acceso fiable, responsable y no discriminatorio a datos de alta calidad con los que entrenar, validar y probar los sistemas de IA. Por ejemplo, en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a datos sanitarios y el entrenamiento, a partir de esos conjuntos de datos, de algoritmos de inteligencia artificial de una manera segura, oportuna, transparente y fiable que respete la privacidad, y contando con la debida gobernanza institucional. Las autoridades competentes pertinentes, incluidas las sectoriales, que proporcionan acceso a datos o lo facilitan también pueden contribuir al suministro de datos de alta calidad orientados a entrenar, validar y probar sistemas de IA.

(46) Para verificar si los sistemas de IA de alto riesgo cumplen los requisitos previstos en el presente Reglamento, resulta esencial disponer de información sobre el modo en que se han desarrollado y sobre su funcionamiento durante todo su ciclo de vida. A tal fin, es preciso llevar registros y disponer de documentación técnica que contenga la información necesaria para evaluar si el sistema de IA en cuestión cumple los requisitos pertinentes. Dicha información debe incluir, en particular, las características, capacidades y limitaciones generales del sistema; los algoritmos; los datos; los procesos de entrenamiento, pruebo y validación empleados, y documentación sobre el sistema de gestión de riesgos pertinente. La documentación técnica debe mantenerse actualizada.

(47) Por otro lado, debe exigirse cierto grado de transparencia respecto de los sistemas de IA de alto riesgo para subsanar la opacidad que puede hacer a algunos de ellos incomprensibles o demasiado complejos para las personas físicas. Los usuarios deben ser capaces de interpretar la información de salida del sistema y de usarla adecuadamente. En consecuencia, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas e incluir

información clara y concisa, en particular sobre los posibles riesgos para los derechos fundamentales y de discriminación, cuando corresponda.

(48) Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que su funcionamiento pueda ser vigilado por personas físicas. A tal fin, el proveedor del sistema debe definir las medidas adecuadas de vigilancia humana antes de su introducción en el mercado o puesta en servicio. Cuando proceda, dichas medidas deben garantizar, en concreto, que el sistema presente limitaciones operativas incorporadas que el propio sistema no pueda desactivar, que responda al operador humano, y que las personas físicas a quienes se haya encomendado la vigilancia humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función.

(49) Los sistemas de IA de alto riesgo deben funcionar de manera consistente durante todo su ciclo de vida y presentar un nivel adecuado de precisión, solidez y ciberseguridad con arreglo al estado de la técnica generalmente reconocido. En este sentido, debe comunicarse a los usuarios el nivel de precisión y los parámetros empleados para medirla.

(50) La solidez técnica es un requisito clave para los sistemas de IA de alto riesgo, que deben ser resilientes a los riesgos asociados a las limitaciones del sistema (p. ej., errores, fallos, incoherencias o situaciones inesperadas), así como a acciones maliciosas que pueden poner en peligro su seguridad y dar lugar a conductas perjudiciales o indeseables por otros motivos. La incapacidad de protegerlos frente a estos riesgos podría tener consecuencias para la seguridad o afectar de manera negativa a los derechos fundamentales, por ejemplo, debido a la adopción de decisiones equivocadas o a que el sistema de IA en cuestión genere una información de salida errónea o sesgada.

(51) La ciberseguridad es fundamental para garantizar que los sistemas de IA resistan a las actuaciones de terceros maliciosos que, aprovechando las vulnerabilidades del sistema, traten de alterar su uso, conducta o funcionamiento o de poner en peligro sus propiedades de seguridad. Los ciberataques contra sistemas de IA pueden dirigirse contra elementos específicos de la IA, como los conjuntos de datos de entrenamiento (p. ej., contaminación de datos) o los modelos entrenados (p. ej., ataques adversarios), o aprovechar las vulnerabilidades de los elementos digitales del sistema de IA o la infraestructura de TIC subyacente. Por lo tanto, para asegurar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas teniendo también en cuenta, cuando proceda, la infraestructura de TIC subyacente.

(52) Como parte de la legislación de armonización de la Unión, conviene que las normas aplicables a la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA de alto riesgo se establezcan en consonancia con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo[51] por el que se establecen los requisitos de acreditación y vigilancia del mercado de los productos; la Decisión

[51] Reglamento (CE) n.º 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) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

n.º 768/2008/CE del Parlamento Europeo y del Consejo[52] sobre un marco común para la comercialización de los productos, y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo[53] relativo a la vigilancia del mercado y la conformidad de los productos (el «nuevo marco legislativo para la comercialización de productos»).

(53) Conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad asociada a la introducción en el mercado o puesta en servicio de un sistema de IA de alto riesgo, con independencia de si dicha persona física o jurídica es o no quien diseñó o desarrolló el sistema.

(54) El proveedor debe instaurar un sistema de gestión de la calidad sólido, velar por que se siga el procedimiento de evaluación de la conformidad necesario, elaborar la documentación pertinente y establecer un sistema sólido de seguimiento posterior a la comercialización. Las autoridades públicas que pongan en servicio sistemas de IA de alto riesgo para su propio uso pueden aprobar y aplicar las normas que regulen el sistema de gestión de la calidad en el marco del sistema de gestión de la calidad adoptado a escala nacional o regional, según proceda, teniendo en cuenta las particularidades del sector y las competencias y la organización de la autoridad pública en cuestión.

(55) Cuando un sistema de IA de alto riesgo que es un componente de seguridad de un producto recogido en una legislación sectorial pertinente del nuevo marco legislativo no se introduzca en el mercado o ponga en servicio independientemente del producto, el fabricante del producto final, según la definición que figure en la legislación pertinente del nuevo marco legislativo, debe cumplir las obligaciones que el presente Reglamento impone al proveedor y, fundamentalmente, asegurarse de que el sistema de IA integrado en el producto final cumpla con los requisitos del presente Reglamento.

(56) Para facilitar la aplicación del presente Reglamento y ofrecer igualdad de condiciones a los operadores, es importante velar por que una persona establecida en la Unión pueda, en cualquier circunstancia, facilitar a las autoridades toda la información necesaria sobre el cumplimiento de un sistema de IA, teniendo en cuenta las distintas formas en que se pueden proporcionar productos digitales. Por lo tanto, cuando no se pueda identificar a un importador, antes de ofrecer sus sistemas de IA en la Unión los proveedores establecidos fuera de su territorio tendrán que designar, mediante un mandato escrito, a un representante autorizado que se encuentre en la Unión.

(57) En consonancia con los principios del nuevo marco legislativo, deben establecerse obligaciones específicas para los operadores económicos pertinentes, como los importadores y los distribuidores, para garantizar la seguridad jurídica y facilitar que dichos operadores cumplan las normativas correspondientes.

(58) Habida cuenta de las características de los sistemas de IA y de los riesgos que su uso puede conllevar para la seguridad y los derechos fundamentales, también en lo que respecta a la necesidad de garantizar la correcta vigilancia del funcionamiento de un

[52] Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82).

[53] Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos 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).

sistema de IA en un contexto real, conviene definir las responsabilidades específicas de los usuarios. En particular, los usuarios deben utilizar los sistemas de IA de alto riesgo conforme a las instrucciones de uso. Además, es preciso definir otras obligaciones en relación con la vigilancia del funcionamiento de los sistemas de IA y con el registro, según proceda.

(59) Conviene prever que el usuario del sistema de IA debe ser la persona física o jurídica, la autoridad pública, la agencia o el organismo de otra índole bajo cuya autoridad se utilice el sistema de IA, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

(60) En vista de la complejidad de la cadena de valor de la inteligencia artificial, los terceros pertinentes, y en especial los involucrados en la venta y el suministro de *software*, herramientas y componentes de *software*, modelos preentrenados y datos, o los proveedores de servicios de red, deben cooperar, según corresponda, con los proveedores y usuarios para que estos cumplan las obligaciones estipuladas en el presente Reglamento y con las autoridades competentes que se mencionan en él.

(61) La normalización debe desempeñar un papel fundamental para proporcionar soluciones técnicas a los proveedores, a fin de garantizar el cumplimiento del presente Reglamento. Los proveedores deben cumplir las normas armonizadas definidas en el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[54] para demostrar su conformidad con los requisitos previstos en el presente Reglamento. No obstante, la Comisión podría adoptar especificaciones técnicas comunes en aquellos ámbitos en los que no existan normas armonizadas o estas sean insuficientes.

(62) Antes de su introducción en el mercado o puesta en servicio, los sistemas de IA de alto riesgo deben someterse a una evaluación de la conformidad que garantice que son altamente fiables.

(63) En el caso de los sistemas de IA de alto riesgo asociados a productos cubiertos por la legislación de armonización vigente en la Unión que sigue el planteamiento del nuevo marco legislativo, conviene que la evaluación de si cumplen o no los requisitos establecidos en el presente Reglamento se enmarque en la evaluación de la conformidad ya prevista en dicha legislación. De este modo, se reducirá al mínimo la carga que deben soportar los operadores y se evitarán posibles duplicidades. Por lo tanto, 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 prevista en la legislación pertinente del nuevo marco legislativo. Este planteamiento se refleja totalmente en la interrelación entre el presente Reglamento y el [Reglamento relativo a las máquinas]. Si bien los requisitos definidos en el presente Reglamento abordan los riesgos de seguridad de los sistemas de IA que desempeñan funciones de seguridad en máquinas, algunos de los requisitos específicos establecidos en el [Reglamento relativo a las máquinas] garantizarán la integración segura del sistema de IA en la máquina general, con el fin de no poner en peligro la seguridad de

[54] Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, 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 por el que se deroga 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).

la máquina en su conjunto. El [Reglamento relativo a las máquinas] aplica la misma definición de «sistema de IA» que el presente Reglamento.

(64) Puesto que los profesionales que realizan la certificación previa a la comercialización tienen una experiencia más amplia en el campo de la seguridad de los productos, y habida cuenta de la diferente naturaleza de los riesgos implicados, procede limitar, al menos en la fase inicial de aplicación del presente Reglamento, el alcance de las evaluaciones de la conformidad realizadas por terceros a los sistemas de IA de alto riesgo que no están asociados a productos. En consecuencia, el proveedor es quien, por norma general, debe llevar a cabo la evaluación de la conformidad de dichos sistemas bajo su propia responsabilidad, con la única excepción de los sistemas de IA que están destinados a utilizarse para la identificación biométrica remota de personas. En el caso de estos últimos, y en la medida en que no estén prohibidos, debe preverse que un organismo notificado participe en la evaluación de la conformidad.

(65) En virtud del presente Reglamento, las autoridades nacionales competentes deben designar a los organismos notificados que realizarán la evaluación externa de la conformidad de los sistemas de IA destinados a utilizarse para la identificación biométrica remota de personas, siempre y cuando cumplan una serie de requisitos, fundamentalmente en lo que respecta a su independencia, sus competencias y la ausencia de conflictos de intereses.

(66) En consonancia con la noción comúnmente establecida de «modificación sustancial» de los productos regulados por la legislación de armonización de la Unión, conviene que un sistema de IA se someta a una nueva evaluación de la conformidad cada vez que se produzca un cambio que pueda afectar al cumplimiento por su parte del presente Reglamento o cuando la finalidad prevista del sistema cambie. Por otro lado, en el caso de los sistemas de IA que siguen «aprendiendo» después de su introducción en el mercado o puesta en servicio (es decir, aquellos que adaptan automáticamente el modo en que desempeñan sus funciones), es necesario establecer normas que indiquen que no deben considerarse modificaciones sustanciales los cambios en el algoritmo y en su funcionamiento que hayan sido predeterminados por el proveedor y se hayan evaluado en el momento de la evaluación de la conformidad.

(67) Los sistemas de IA de alto riesgo deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

(68) En determinadas condiciones, la rápida disponibilidad de tecnologías innovadoras puede ser crucial para la salud y la seguridad de las personas y para la sociedad en su conjunto. Por consiguiente, resulta oportuno que los Estados miembros puedan autorizar, por motivos excepcionales de seguridad pública o con vistas a proteger la vida y la salud de personas físicas y la propiedad industrial y mercantil, la introducción en el mercado o la puesta en servicio de sistemas de IA que no hayan sido sometidos a una evaluación de la conformidad.

(69) Con el objetivo de facilitar la labor de la Comisión y de los Estados miembros en el ámbito de la inteligencia artificial, así como de incrementar la transparencia de cara al público, debe exigirse a los proveedores de sistemas de IA de alto riesgo que no están asociados a productos que entran dentro del ámbito de aplicación de la legislación de armonización vigente en la Unión que registren dichos sistemas en una base de datos

de la UE, de cuya creación y gestión se encargará la Comisión. La Comisión debe ser la responsable del tratamiento de dicha base de datos, de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[55]. Con vistas a garantizar la funcionalidad plena de la base de datos una vez que esté en funcionamiento, el procedimiento para su establecimiento debe incluir la elaboración de especificaciones funcionales por parte de la Comisión y la redacción de un informe de auditoría independiente.

(70) Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden conllevar riesgos específicos de suplantación o falsificación, con independencia de si son clasificados como de alto riesgo o no. Por consiguiente, el uso de estos sistemas debe estar sujeto, en determinadas circunstancias, a obligaciones de transparencia específicas, sin perjuicio de los requisitos y las obligaciones aplicables a los sistemas de IA de alto riesgo. En particular, es preciso notificar a las personas físicas que están interactuando con un sistema de IA, salvo que sea evidente por las circunstancias y el contexto de uso, e informarlas cuando estén expuestas a un sistema de reconocimiento de emociones o a un sistema de categorización biométrica. Esta información y estas notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad. Además, los usuarios que utilicen un sistema de IA para generar o manipular imágenes, archivos de audio o vídeos que se asemejen notablemente a personas, lugares o sucesos reales y puedan inducir erróneamente a una persona a pensar que son auténticos, deben comunicar que estos han sido creados o manipulados de manera artificial etiquetando el contenido generado por la inteligencia artificial como corresponda e indicando su origen artificial.

(71) La inteligencia artificial es una familia de tecnologías de rápida evolución que requiere nuevas formas de vigilancia regulatoria y un espacio seguro para la experimentación, así como que se garantice la innovación responsable y la integración de salvaguardias y medidas de reducción del riesgo adecuadas. Para conseguir un marco jurídico que favorezca la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones, conviene animar a las autoridades nacionales competentes de uno o varios Estados miembros a que establezcan espacios controlados de pruebas para la inteligencia artificial que faciliten el desarrollo y la prueba de sistemas de IA innovadores bajo una estricta vigilancia regulatoria antes de su introducción en el mercado o puesta en servicio.

(72) Los espacios controlados de pruebas deben tener los objetivos de impulsar la innovación en el ámbito de la IA estableciendo un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización, con vistas a garantizar que los sistemas de IA innovadores cumplan lo dispuesto en el presente Reglamento y en otra legislación pertinente de la Unión y los Estados miembros; de redoblar la seguridad jurídica de que gozan los innovadores y favorecer la vigilancia de las autoridades competentes y su entendimiento de las oportunidades, los riesgos emergentes y las consecuencias del uso de la IA; y de acelerar el acceso a los mercados eliminando las barreras para las pequeñas y medianas empresas (pymes) y las empresas emergentes, entre otras medidas. Para garantizar una aplicación uniforme en toda la Unión y conseguir economías de escala, resulta oportuno establecer normas

[55] 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).

comunes para la creación de espacios controlados de pruebas, así como un marco para la cooperación entre las autoridades pertinentes implicadas en la supervisión de dichos espacios. El presente Reglamento debe sentar la base jurídica para utilizar los datos personales recabados para otros fines en el desarrollo de determinados sistemas de IA en aras del interés público en el espacio controlado de pruebas para la IA, con arreglo al artículo 6, apartado 4, del Reglamento (UE) 2016/679 y al artículo 6 del Reglamento (UE) 2018/1725, y sin perjuicio de lo dispuesto en el artículo 4, apartado 2, de la Directiva (UE) 2016/680. Los participantes en el espacio de pruebas deben proporcionar las salvaguardias adecuadas y cooperar con las autoridades competentes, entre otras cosas, siguiendo sus indicaciones y actuando con rapidez y de buena fe para mitigar cualquier posible alto riesgo para la seguridad y los derechos fundamentales que pueda surgir durante el desarrollo y la experimentación en dicho espacio. Cuando decidan si imponen o no una multa administrativa en virtud del artículo 83, apartado 2, del Reglamento 2016/679 y del artículo 57 de la Directiva 2016/680, las autoridades competentes deben tener en cuenta la conducta de los participantes en el espacio de pruebas.

(73) Para promover y proteger la innovación, es importante tener en particular consideración los intereses de los proveedores y los usuarios de sistemas de IA a pequeña escala. A tal fin, los Estados miembros deben desarrollar iniciativas en materia de concienciación y comunicación de información, entre otros aspectos, dirigidas a dichos operadores. Asimismo, los organismos notificados deben tener en cuenta las necesidades y los intereses específicos de los proveedores a pequeña escala cuando establezcan las tasas aplicables a las evaluaciones de la conformidad. Los costes de traducción ligados a la documentación obligatoria y a la comunicación con las autoridades pueden ser considerables para los proveedores y otros operadores, en especial para los de menor tamaño. En la medida de lo posible, los Estados miembros deben procurar que una de las lenguas en las que acepten que los proveedores presenten la documentación pertinente y que pueda usarse para la comunicación con los operadores sea ampliamente conocida por el mayor número posible de usuarios transfronterizos.

(74) Con vistas a reducir al mínimo los riesgos para la aplicación derivados de la falta de conocimientos y experiencia en el mercado, y con el objetivo de facilitar que los proveedores y los organismos notificados cumplan las obligaciones que les impone el presente Reglamento, la plataforma de IA a la carta, los centros de innovación digital europeos y los centros de ensayo y experimentación establecidos por la Comisión y los Estados miembros a escala nacional o de la UE deben, en la medida de lo posible, contribuir a la aplicación de este Reglamento. En concreto, pueden proporcionar asistencia técnica y científica a los proveedores y organismos notificados en sus respectivas misiones y esferas de competencia.

(75) Resulta adecuado que la Comisión facilite, en la medida de lo posible, el acceso a los centros de ensayo y experimentación a organismos, grupos o laboratorios que se hayan establecido o acreditado conforme a la legislación de armonización pertinente de la Unión y que realicen tareas en el marco de la evaluación de la conformidad de productos o dispositivos cubiertos por dicha legislación. Tal es el caso de los paneles de expertos, los laboratorios de expertos y los laboratorios de referencia en el ámbito de los productos sanitarios, conforme al Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746.

(76) Debe establecerse un Comité Europeo de Inteligencia Artificial que facilite la aplicación fluida, efectiva y armonizada del presente Reglamento. Dicho Comité

deberá encargarse de diversas tareas de asesoramiento. Entre otras cosas, deberá emitir dictámenes, recomendaciones, informes de asesoramiento u orientaciones sobre asuntos relacionados con la aplicación de este Reglamento, en particular en lo que respecta a las especificaciones técnicas o las normas existentes en relación con los requisitos previstos en el presente Reglamento, y asesorar y apoyar a la Comisión en cuestiones específicas vinculadas a la inteligencia artificial.

(77) Los Estados miembros desempeñan un papel clave en la aplicación y ejecución de este Reglamento. En este sentido, cada Estado miembro debe designar a una o varias autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Con el fin de incrementar la eficiencia en términos de organización en los Estados miembros y establecer un punto de contacto oficial con el público y otros homólogos en los Estados miembros y la Unión, una autoridad nacional de cada Estado miembro debe ser designada autoridad nacional de supervisión.

(78) Todos los proveedores de sistemas de IA de alto riesgo deben contar con un sistema de seguimiento posterior a la comercialización, con vistas a garantizar que puedan tener en cuenta la experiencia con el uso de esos sistemas de cara a mejorar los suyos y el proceso de diseño y desarrollo o de que puedan adoptar las medidas correctoras necesarias en el momento oportuno. Este sistema es también fundamental para asegurar que los posibles riesgos derivados de los sistemas de IA que siguen «aprendiendo» tras su introducción en el mercado o puesta en servicio se aborden de un modo más eficiente y oportuno. En este contexto, también procede exigir a los proveedores que cuenten con un sistema para comunicar a las autoridades pertinentes cualquier incidente grave o incumplimiento del Derecho interno y de la Unión que proteja los derechos fundamentales asociado al uso de sus sistemas de IA.

(79) Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y obligaciones previstos en el presente Reglamento, que constituye legislación armonizada de la Unión, debe aplicarse en su totalidad el sistema relativo a la vigilancia del mercado y la conformidad de los productos establecido por el Reglamento (UE) 2019/1020. Cuando sea necesario para el cumplimiento de su mandato, las autoridades o los organismos públicos nacionales que supervisen la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de igualdad, también deben tener acceso a la documentación que se cree en virtud del presente Reglamento.

(80) La legislación de la Unión relativa a los servicios financieros contiene normas y requisitos en materia de gobernanza interna y gestión de riesgos que las entidades financieras reguladas deben cumplir durante la prestación de dichos servicios, y también cuando utilicen sistemas de IA. Para garantizar la aplicación y ejecución coherentes de las obligaciones previstas en el presente Reglamento, así como de las normas y los requisitos oportunos de la legislación de la Unión relativa a los servicios financieros, se ha de designar a las autoridades encargadas de supervisar y ejecutar dicha legislación, y en particular, cuando proceda, al Banco Central Europeo, como las autoridades competentes encargadas de supervisar la aplicación del presente Reglamento, también de cara a las actividades de vigilancia del mercado, en relación con los sistemas de IA proporcionados o usados por entidades financieras reguladas y supervisadas. Con vistas a aumentar la coherencia entre el presente Reglamento y las normas aplicables a las entidades de crédito reguladas por la Directiva 2013/36/UE del

Parlamento Europeo y del Consejo[56], conviene igualmente integrar el procedimiento de evaluación de la conformidad y algunas de las obligaciones procedimentales de los proveedores relativas a la gestión de riesgos, el seguimiento posterior a la comercialización y la documentación en las obligaciones y los procedimientos vigentes con arreglo a la Directiva 2013/36/UE. Para evitar solapamientos, también se deben contemplar excepciones limitadas en relación con el sistema de gestión de la calidad de los proveedores y la obligación de seguimiento impuesta a los usuarios de sistemas de IA de alto riesgo, en la medida en que estas se apliquen a las entidades de crédito reguladas por la Directiva 2013/36/UE.

(81) El desarrollo de sistemas de IA que no sean sistemas de IA de alto riesgo conforme a los requisitos estipulados en el presente Reglamento puede favorecer la adopción más amplia de inteligencia artificial fiable en la Unión. Se debe instar a los proveedores de sistemas de IA que no son de alto riesgo a crear códigos de conducta destinados a impulsar la aplicación voluntaria de los requisitos que son obligatorios para los sistemas de IA de alto riesgo. Asimismo, se les debe animar a aplicar, con carácter voluntario, requisitos adicionales relativos, por ejemplo, a la sostenibilidad medioambiental, la accesibilidad para las personas con discapacidad, la participación de las partes interesadas en el diseño y el desarrollo de sistemas de IA, y la diversidad de los equipos de desarrollo. La Comisión podría formular iniciativas, también de carácter sectorial, encaminadas a facilitar la reducción de las barreras técnicas que obstaculizan el intercambio transfronterizo de datos para el desarrollo de IA, también en relación con la infraestructura de acceso a los datos y a la interoperabilidad semántica y técnica de distintos tipos de datos.

(82) Es importante que los sistemas de IA asociados a productos que el presente Reglamento no considera de alto riesgo y que, por lo tanto, no están obligados a cumplir los requisitos establecidos en él sean, no obstante, seguros una vez introducidos en el mercado o puestos en servicio. Para contribuir a este objetivo, se aplicaría, como red de seguridad, la Directiva 2001/95/CE del Parlamento Europeo y del Consejo[57].

(83) Todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones, con vistas a garantizar la cooperación fiable y constructiva de las autoridades competentes en la Unión y a escala nacional.

(84) Los Estados miembros deben tomar todas las medidas necesarias para asegurarse de que se apliquen las disposiciones del presente Reglamento, incluso estableciendo sanciones efectivas, proporcionadas y disuasorias para las infracciones que se cometan. En el caso de ciertas infracciones concretas, los Estados miembros deben tener en cuenta los márgenes y criterios establecidos en el presente Reglamento. El Supervisor Europeo de Protección de Datos debe estar facultado para imponer multas administrativas a las instituciones, las agencias y los organismos de la Unión comprendidos en el ámbito de aplicación del presente Reglamento.

---

56 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).

57 Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (DO L 11 de 15.1.2002, p. 4).

(85) Con el objetivo de garantizar que el marco reglamentario pueda adaptarse cuando sea necesario, debe delegarse en la Comisión el poder para adoptar actos previsto en el artículo 290 del TFUE, de modo que pueda modificar las técnicas y estrategias para definir sistemas de IA mencionadas en el anexo I, la legislación de armonización de la Unión indicada en el anexo II, la lista de sistemas de IA de alto riesgo del anexo III, las disposiciones relativas a la documentación técnica que figuran en el anexo IV, el contenido de la declaración UE de conformidad del anexo V, las disposiciones referentes a los procedimientos de evaluación de la conformidad que figuran en los anexos VI y VII, y las disposiciones que estipulan a qué sistemas de IA de alto riesgo debe aplicarse el procedimiento de evaluación de la conformidad basado en la evaluación del sistema de gestión de la calidad y en la evaluación de la documentación técnica. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016[58]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación 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 ocupen de la preparación de actos delegados.

(86) Para garantizar que la aplicación del presente Reglamento se efectúe en condiciones uniformes, deben concederse competencias de ejecución a la Comisión, que debe ejercerlas de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[59].

(87) Dado que el objetivo del presente Reglamento no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones y efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(88) El presente Reglamento debe aplicarse a partir del ... [*OP – introdúzcase la fecha indicada en el art. 85*]. No obstante, la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad debe estar operativa antes de esa fecha, por lo que las disposiciones relativas a los organismos notificados y la estructura de gobernanza deben ser aplicables a partir del ... [*OP – introdúzcase la fecha correspondiente a tres meses a contar desde la entrada en vigor del presente Reglamento*]. Asimismo, los Estados miembros deben establecer y poner en conocimiento de la Comisión las normas referentes a las sanciones, incluidas las multas administrativas, y asegurarse de que para la fecha de aplicación del presente Reglamento se apliquen de manera adecuada y efectiva. De este modo, las disposiciones relativas a las sanciones deben aplicarse a partir del [*OP – introdúzcase la fecha correspondiente a doce meses a contar desde la entrada en vigor del presente Reglamento*].

---

58 DO L 123 de 12.5.2016, p. 1.

59 Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(89) El Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos fueron consultados de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725, y emitieron un dictamen sobre […].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1
Objeto

El presente Reglamento establece:

a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial («sistemas de IA») en la Unión;

b) prohibiciones 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 armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica, así como a los sistemas de IA usados para generar o manipular imágenes, archivos de audio o vídeos;

e) normas sobre el control y la vigilancia del mercado.

Artículo 2
Ámbito de aplicación

1. El presente Reglamento es aplicable a:

a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión, con independencia de si dichos proveedores están establecidos en la Unión o en un tercer país;

b) los usuarios de sistemas de IA que se encuentren en la Unión;

c) los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión.

2. A los sistemas de IA de alto riesgo que sean componentes de seguridad de productos o sistemas, o que sean en sí mismos productos o sistemas, comprendidos en el ámbito de aplicación de los actos que figuran a continuación, únicamente se les aplicará el artículo 84 del presente Reglamento:

a) el Reglamento (CE) n.º 300/2008;

b) el Reglamento (UE) n.º 167/2013;

c) el Reglamento (UE) n.º 168/2013;

d) la Directiva 2014/90/UE;

e) la Directiva (UE) 2016/797;

f) el Reglamento (UE) 2018/858;

g) el Reglamento (UE) 2018/1139;

h) el Reglamento (UE) 2019/2144.

3. El presente Reglamento no se aplicará a los sistemas de IA desarrollados o utilizados exclusivamente con fines militares.

4. El presente Reglamento no se aplicará a las autoridades públicas de terceros países ni a las organizaciones internacionales que entren dentro del ámbito de aplicación de este Reglamento conforme al apartado 1 cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos internacionales con fines de aplicación de la ley y cooperación judicial con la Unión o con uno o varios Estados miembros.

5. El presente Reglamento no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II, sección IV, de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo[60] [*que deben sustituirse por las disposiciones correspondientes de la Ley de Servicios Digitales*].

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «Sistema de inteligencia artificial (sistema de IA)»: el *software* que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

2) «Proveedor»: toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita.

3) «Proveedor a pequeña escala»: todo proveedor que sea una microempresa o una pequeña empresa en el sentido de la Recomendación 2003/361/CE de la Comisión[61].

4) «Usuario»: toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

5) «Representante autorizado»: toda persona física o jurídica establecida en la Unión que haya recibido el mandato por escrito de un proveedor de un sistema de IA para

60 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).

61 Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor.

6) «Importador»: toda persona física o jurídica establecida en la Unión que introduzca en el mercado o ponga en servicio 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»: toda persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercializa un sistema de IA en el mercado de la Unión sin influir sobre sus propiedades.

8) «Operador»: el proveedor, el usuario, el representante autorizado, el importador y el distribuidor.

9) «Introducción en el mercado»: la primera comercialización en el mercado de la Unión de un sistema de IA.

10) «Comercialización»: todo suministro de un sistema de IA para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, ya se produzca el suministro de manera remunerada o gratuita.

11) «Puesta en servicio»: el suministro de un sistema de IA para su primer uso directamente al usuario o para uso propio en el mercado de la Unión de acuerdo con su finalidad prevista.

12) «Finalidad prevista»: el uso para el que un proveedor concibe un sistema de IA, incluido el contexto y las condiciones de uso concretas, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica.

13) «Uso indebido razonablemente previsible»: la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas razonablemente previsible.

14) «Componente de seguridad de un producto o sistema»: un componente de un producto o un sistema que cumple una función de seguridad para dicho producto o sistema, o cuyo fallo o defecto de funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes.

15) «Instrucciones de uso»: la información facilitada por el proveedor para informar al usuario, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA, lo que incluye el entorno geográfico, conductual o funcional específico en el que se pretende utilizar el sistema de IA de alto riesgo.

16) «Recuperación de un sistema de IA»: toda medida encaminada a conseguir que el proveedor recupere un sistema de IA puesto a disposición de los usuarios.

17) «Retirada de un sistema de IA»: toda medida destinada a impedir la distribución, la exposición y la oferta de un sistema de IA.

18) «Funcionamiento de un sistema de IA»: la capacidad de un sistema de IA para alcanzar su finalidad prevista.

19) «Autoridad notificante»: la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su seguimiento.

20) «Evaluación de la conformidad»: el proceso por el que se verifica si se cumplen los requisitos establecidos en el título III, capítulo 2, del presente Reglamento en relación con un sistema de IA.

21) «Organismo de evaluación de la conformidad»: un organismo independiente que desempeña actividades de evaluación de la conformidad, entre las que figuran la prueba, la certificación y la inspección.

22) «Organismo notificado»: un organismo de evaluación de la conformidad designado con arreglo al presente Reglamento y otra legislación de armonización pertinente de la Unión.

23) «Modificación sustancial»: un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que afecte al cumplimiento por su parte de los requisitos establecidos en el título III, capítulo 2, del presente Reglamento o que provoque la modificación de la finalidad prevista para la que se ha evaluado al sistema de IA en cuestión.

24) «Marcado CE de conformidad» o «marcado CE»: un marcado con 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 otra legislación de la Unión aplicable que armonice las condiciones para la comercialización de productos (la «legislación de armonización de la Unión») y prevea su colocación.

25) «Seguimiento posterior a la comercialización»: todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recopilar y examinar de forma proactiva la experiencia obtenida con el uso de sistemas de IA que introducen en el mercado o ponen en servicio, con objeto de detectar la posible necesidad de aplicar inmediatamente cualquier tipo de medida correctora o preventiva que resulte necesaria.

26) «Autoridad de vigilancia del mercado»: la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020.

27) «Norma armonizada»: una norma europea conforme a la definición que figura en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012.

28) «Especificaciones comunes»: un documento, distinto de una norma, con soluciones técnicas que proponen una forma de cumplir determinados requisitos y obligaciones establecidos en el presente Reglamento.

29) «Datos de entrenamiento»: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables, entre los que se incluyen los pesos de una red neuronal.

30) «Datos de validación»: los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje, entre otras cosas, para evitar el sobreajuste. El conjunto de datos de validación puede ser un conjunto de datos independiente o formar parte del conjunto de datos de entrenamiento, ya sea como una división fija o variable.

31) «Datos de prueba»: los datos usados para proporcionar una evaluación independiente del sistema de IA entrenado y validado, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio.

32) «Datos de entrada»: los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce la información de salida.

33) «Datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

34) «Sistema de reconocimiento de emociones»: un sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos.

35) «Sistema de categorización biométrica»: un sistema de IA destinado a asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política, en función de sus datos biométricos.

36) «Sistema de identificación biométrica remota»: un sistema de IA destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada.

37) «Sistema de identificación biométrica remota "en tiempo real"»: un sistema de identificación biométrica remota en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión.

38) «Sistema de identificación biométrica remota "en diferido"»: todo sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota «en tiempo real».

39) «Espacio de acceso público»: cualquier lugar físico accesible para el público, con independencia de que deban cumplirse determinadas condiciones para acceder a él.

40) «Autoridad encargada de la aplicación de la ley»:

   a) toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública; o

   b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública.

41) «Aplicación de la ley»: las actividades realizadas por las autoridades encargadas de la aplicación de la ley para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública.

42) «Autoridad nacional de supervisión»: la autoridad a la que un Estado miembro asigna la responsabilidad de ejecutar y aplicar el presente Reglamento, coordinar las actividades encomendadas a dicho Estado miembro, actuar como el punto de

contacto único para la Comisión, y representar al Estado miembro en cuestión ante el Comité Europeo de Inteligencia Artificial.

43) «Autoridad nacional competente»: la autoridad nacional de supervisión, la autoridad notificante y la autoridad de vigilancia del mercado.

44) «Incidente grave»: todo incidente que, directa o indirectamente, tenga, pueda haber tenido o pueda tener alguna de las siguientes consecuencias:

a) el fallecimiento de una persona o daños graves para su salud, para los bienes o para el medio ambiente;

b) una alteración grave e irreversible de la gestión y el funcionamiento de infraestructura crítica.

Artículo 4
Modificaciones del anexo I

Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar la lista de técnicas y estrategias que figura en el anexo I, con miras a adaptar dicha lista a la evolución del mercado y los avances tecnológicos sobre la base de características que sean similares a las técnicas y las estrategias incluidas en ella.

TÍTULO II

PRÁCTICAS DE INTELIGENCIA ARTIFICIAL PROHIBIDAS

Artículo 5

1. Estarán prohibidas las siguientes prácticas de inteligencia artificial:

a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.

b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.

c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

d) El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;

iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo[62], para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para conseguir cualquiera de los objetivos mencionados en el apartado 1, letra d), tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra d), cumplirá salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales.

3. Con respecto al apartado 1, letra d), y el apartado 2, cualquier uso concreto de un sistema de identificación biométrica remota «en tiempo real» en un espacio de acceso público con fines de aplicación de la ley estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema, que la otorgarán previa solicitud motivada y de conformidad con las normas detalladas del Derecho interno mencionadas en el apartado 4. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema

[62] 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).

antes de obtener la autorización correspondiente, que podrá solicitarse durante el uso o después de este.

La autoridad judicial o administrativa competente únicamente concederá la autorización cuando esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos que figuran en el apartado 1, letra d), el cual se indicará en la solicitud. Al pronunciarse al respecto, la autoridad judicial o administrativa competente tendrá en cuenta los aspectos mencionados en el apartado 2.

4. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra d), y los apartados 2 y 3. A tal fin, tendrán que establecer en sus respectivos Derechos internos las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión de estas. Dichas normas especificarán también para cuáles de los objetivos enumerados en el apartado 1, letra d), y en su caso en relación con cuáles de los delitos indicados en su inciso iii), se podrá autorizar que las autoridades competentes utilicen esos sistemas con fines de aplicación de la ley.

TÍTULO III

SISTEMAS DE IA DE ALTO RIESGO

CAPÍTULO 1

CLASIFICACIÓN DE LOS SISTEMAS DE IA COMO SISTEMAS DE ALTO RIESGO

Artículo 6
Reglas de clasificación para los sistemas de IA de alto riesgo

1. Un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación, con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b):

   a) el sistema de IA está destinado a ser utilizado como componente de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión que se indica en el anexo II, o es en sí mismo uno de dichos productos;

   b) conforme a la legislación de armonización de la Unión que se indica en el anexo II, el producto del que el sistema de IA es componente de seguridad, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio.

2. Además de los sistemas de IA de alto riesgo mencionados en el apartado 1, también se considerarán de alto riesgo los sistemas de IA que figuran en el anexo III.

Artículo 7
Modificaciones del anexo III

1. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar la lista del anexo III mediante la adición de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

   a) los sistemas de IA estén destinados a utilizarse en cualquiera de los ámbitos que figuran en los puntos 1 a 8 del anexo III; y

   b) los sistemas de IA conlleven el riesgo de causar un perjuicio a la salud y la seguridad, o el riesgo de tener repercusiones negativas para los derechos fundamentales, cuya gravedad y probabilidad sean equivalentes o mayores a las de los riesgos de perjuicio o de repercusiones negativas asociados a los sistemas de IA de alto riesgo que ya se mencionan en el anexo III.

2. Cuando, a los efectos del apartado 1, se evalúe si un sistema de IA conlleva el riesgo de causar un perjuicio a la salud y la seguridad o el riesgo de tener repercusiones negativas para los derechos fundamentales que sea equivalente o mayor a los riesgos de perjuicio asociados a los sistemas de IA de alto riesgo que ya se mencionan en el anexo III, la Comisión tendrá en cuenta los criterios siguientes:

   a) la finalidad prevista del sistema de IA;

   b) la medida en que se haya utilizado o sea probable que se utilice un sistema de IA;

   c) la medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad, haya tenido repercusiones negativas para los derechos fundamentales o haya dado lugar a problemas importantes en relación con la materialización de dicho perjuicio o dichas repercusiones negativas, según demuestren los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes;

   d) el posible alcance de dicho perjuicio o dichas repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a una gran variedad de personas;

   e) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan de la información de salida generada con un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicha información;

   f) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del usuario de un sistema de IA, en particular debido a un desequilibrio en cuanto al poder o los conocimientos que ambos poseen, sus circunstancias económicas o sociales, o su edad;

   g) la medida en que sea fácil revertir la información de salida generada con un sistema de IA, habida cuenta de que no se debe considerar que la información de salida que afecta a la salud o la seguridad de las personas es fácil de revertir;

   h) la medida en que la legislación vigente en la Unión establezca:

      i) medidas de compensación efectivas en relación con los riesgos que conlleva un sistema de IA, con exclusión de las acciones por daños y perjuicios;

ii) medidas efectivas para prevenir o reducir notablemente esos riesgos.

CAPÍTULO 2

REQUISITOS PARA LOS SISTEMAS DE IA DE ALTO RIESGO

Artículo 8
Cumplimiento de los requisitos

1. Los sistemas de IA de alto riesgo cumplirán los requisitos que se definen en el presente capítulo.

2. A la hora de verificar su cumplimiento se tendrán en cuenta la finalidad prevista del sistema de IA de alto riesgo y el sistema de gestión de riesgos al que se refiere el artículo 9.

Artículo 9
Sistema de gestión de riesgos

1. Se establecerá, implantará, documentará y mantendrá un sistema de gestión de riesgos asociado a los sistemas de IA de alto riesgo.

2. El sistema de gestión de riesgos consistirá en un proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, el cual requerirá actualizaciones sistemáticas periódicas. Constará de las siguientes etapas:

   a) la identificación y el análisis de los riesgos conocidos y previsibles vinculados a cada sistema de IA de alto riesgo;

   b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo en cuestión se utilice conforme a su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible;

   c) la evaluación de otros riesgos que podrían surgir a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización al que se refiere el artículo 61;

   d) la adopción de medidas oportunas de gestión de riesgos con arreglo a lo dispuesto en los apartados siguientes.

3. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), darán la debida consideración a los efectos y las posibles interacciones derivados de la aplicación combinada de los requisitos estipulados en el presente capítulo 2. Asimismo, tendrán en cuenta el estado actual de la técnica generalmente reconocido, que, entre otras fuentes, está reflejado en las normas armonizadas o las especificaciones comunes pertinentes.

4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), considerarán aceptables los riesgos residuales asociados a cada peligro, así como el riesgo residual general de los sistemas de IA de alto riesgo, siempre que el sistema de IA de alto riesgo de que se trate se utilice conforme a su finalidad prevista o que se le dé un uso indebido razonablemente previsible. Se informará al usuario de dichos riesgos residuales.

   A la hora de determinar cuáles son las medidas de gestión de riesgos más adecuadas, se procurará:

a) eliminar o reducir los riesgos en la medida en que sea posible mediante un diseño y un desarrollo adecuados;

b) implantar, cuando proceda, unas medidas de mitigación y control apropiadas en relación con los riesgos que no puedan eliminarse;

c) proporcionar la información oportuna conforme al artículo 13, en particular en relación con los riesgos mencionados en el apartado 2, letra b), del presente artículo y, cuando proceda, impartir formación a los usuarios.

Cuando se eliminen o reduzcan los riesgos asociados a la utilización del sistema de IA de alto riesgo, se tendrán en la debida consideración los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el usuario, así como el entorno en el que está previsto que se utilice el sistema.

5. Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de un modo adecuado para su finalidad prevista y cumplen los requisitos establecidos en el presente capítulo.

6. Los procedimientos de prueba serán adecuados para alcanzar la finalidad prevista del sistema de IA y no excederán de lo necesario para ello.

7. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en todo caso, antes de su introducción en el mercado o puesta en servicio. Los ensayos se realizarán a partir de parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo de que se trate.

8. Cuando se implante el sistema de gestión de riesgos descrito en los apartados 1 a 7, se prestará especial atención a la probabilidad de que menores accedan al sistema de IA de alto riesgo de que se trate o se vean afectados por él.

9. En el caso de las entidades de crédito reguladas por la Directiva 2013/36/UE, los aspectos descritos en los apartados 1 a 8 formarán parte de los procedimientos de gestión de riesgos que estas establezcan conforme al artículo 74 de dicha Directiva.

Artículo 10
Datos y gobernanza de datos

1. Los sistemas de IA de alto riesgo que utilizan técnicas que implican el entrenamiento de modelos con datos se desarrollarán a partir de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad expuestos en los apartados 2 a 5.

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas adecuadas de gobernanza y gestión de datos. Dichas prácticas se centrarán, en particular, en:

a) la elección de un diseño adecuado;

b) la recopilación de datos;

c) las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, el enriquecimiento y la agregación;

d) la formulación de los supuestos pertinentes, fundamentalmente en lo que respecta a la información que, ateniéndose a ellos, los datos miden y representan;

e) la evaluación previa de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios;

f) el examen atendiendo a posibles sesgos;

g) la detección de posibles lagunas o deficiencias en los datos y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes y representativos, carecerán de errores y estarán completos. Asimismo, tendrán las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema de IA de alto riesgo, cuando proceda. Los conjuntos de datos podrán reunir estas características individualmente para cada dato o para una combinación de estos.

4. Los conjuntos de datos de entrenamiento, validación y prueba tendrán en cuenta, en la medida necesaria en función de su finalidad prevista, las características o elementos particulares del contexto geográfico, conductual o funcional específico en el que se pretende utilizar el sistema de IA de alto riesgo.

5. En la medida en que sea estrictamente necesario para garantizar la vigilancia, la detección y la corrección de los sesgos asociados a los sistemas de IA de alto riesgo, los proveedores de dichos sistemas podrán tratar las categorías especiales de datos personales que se mencionan en 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, ofreciendo siempre las salvaguardias adecuadas para los derechos y las libertades fundamentales de las personas físicas, lo que incluye establecer limitaciones técnicas a la reutilización y la utilización de las medidas de seguridad y protección de la privacidad más recientes, tales como la seudonimización o el cifrado, cuando la anonimización pueda afectar significativamente al objetivo perseguido.

6. Se emplearán prácticas adecuadas de gobernanza y gestión de datos para desarrollar sistemas de IA de alto riesgo distintos de aquellos que utilizan técnicas que implican el entrenamiento de modelos, con vistas a garantizar que dichos sistemas de IA de alto riesgo cumplan lo dispuesto en el apartado 2.

Artículo 11
Documentación técnica

1. La documentación técnica de un sistema de IA de alto riesgo se preparará antes de su introducción en el mercado o puesta en servicio, y se mantendrá actualizada.

   La documentación técnica se redactará de modo que demuestre que el sistema de IA de alto riesgo cumple los requisitos establecidos en el presente capítulo y proporcionará a las autoridades nacionales competentes y los organismos notificados toda la información que necesiten para evaluar si el sistema de IA de que se trate cumple dichos requisitos. Contendrá, como mínimo, los elementos contemplados en el anexo IV.

2. Cuando se introduzca en el mercado o se ponga en servicio un sistema de IA de alto riesgo asociado a un producto al que se apliquen los actos legislativos mencionados

en el anexo II, sección A, se elaborará una única documentación técnica que contenga toda la información estipulada en el anexo IV, así como la información que exijan dichos actos legislativos.

3. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar el anexo IV cuando sea necesario para garantizar que, en vista de los avances técnicos, la documentación técnica proporcione toda la información necesaria para evaluar si el sistema cumple los requisitos establecidos en el presente capítulo.

Artículo 12
Registros

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán con capacidades que permitan registrar automáticamente eventos («archivos de registro») mientras están en funcionamiento. Estas capacidades de registro se ajustarán a las normas o las especificaciones comunes reconocidas.

2. Las capacidades de registro garantizarán un nivel de trazabilidad del funcionamiento del sistema de IA durante su ciclo de vida que resulte adecuado para la finalidad prevista del sistema.

3. En particular, las capacidades de registro permitirán controlar el funcionamiento del sistema de IA de alto riesgo en lo que respecta a la aparición de situaciones que puedan hacer que este sistema presente un riesgo, en el sentido del artículo 65, apartado 1, o dar lugar a una modificación sustancial, y facilitarán el seguimiento posterior a la comercialización al que se refiere el artículo 61.

4. En el caso de los sistemas de IA de alto riesgo que figuran en el punto 1, letra a), del anexo III, las capacidades de registro incluirán, como mínimo:

   a) un registro del período de cada uso del sistema (la fecha y la hora de inicio y la fecha y la hora de finalización 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 con los que la búsqueda ha arrojado una correspondencia;

   d) la identificación de las personas físicas implicadas en la verificación de los resultados que se mencionan en el artículo 14, apartado 5.

Artículo 13
Transparencia y comunicación de información a los usuarios

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el usuario y el proveedor cumplan las obligaciones oportunas previstas en el capítulo 3 del presente título.

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

3. La información a que se refiere el apartado 2 especificará:

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

b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, y en particular:

i) su finalidad prevista;

ii) el nivel de precisión, solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse de este, así como las circunstancias conocidas o previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado;

iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales;

iv) su funcionamiento en relación con las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema;

v) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA;

c) los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso;

d) las medidas de vigilancia humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios;

e) la vida útil prevista del sistema de IA de alto riesgo, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a la actualización del *software*.

Artículo 14
Vigilancia humana

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada, entre otras cosas.

2. El objetivo de la vigilancia humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando un sistema de IA de alto riesgo se utiliza conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persisten a pesar de aplicar otros requisitos establecidos en el presente capítulo.

3. La vigilancia humana se garantizará de una de las siguientes maneras o de ambas:

a) el proveedor definirá las medidas de vigilancia humana y, cuando sea técnicamente viable, las integrará en el sistema de IA de alto riesgo antes de su introducción en el mercado o puesta en servicio;

b) el proveedor definirá las medidas de vigilancia humana, que serán adecuadas para que las lleve a cabo el usuario, antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio.

4. Las medidas mencionadas en el apartado 3 permitirán que las personas a quienes se encomiende la vigilancia humana puedan, en función de las circunstancias:

a) entender por completo las capacidades y limitaciones del sistema de IA de alto riesgo y controlar debidamente su funcionamiento, de modo que puedan detectar indicios de anomalías, problemas de funcionamiento y comportamientos inesperados y ponerles solución lo antes posible;

b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en la información de salida generada por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión;

c) interpretar correctamente la información de salida del sistema de IA de alto riesgo, teniendo en cuenta en particular las características del sistema y las herramientas y los métodos de interpretación disponibles;

d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o desestimar, invalidar o revertir la información de salida que este genere;

e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema accionando un botón específicamente destinado a tal fin o mediante un procedimiento similar.

5. En el caso de los sistemas de IA mencionados en el punto 1, letra a), del anexo III, las medidas que figuran en el apartado 3 garantizarán además que el usuario no actúe ni tome ninguna decisión sobre la base de la identificación generada por el sistema, salvo que un mínimo de dos personas físicas la hayan verificado y confirmado.

Artículo 15
Precisión, solidez y ciberseguridad

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que, en vista de su finalidad prevista, alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera consistente en esos sentidos durante todo su ciclo de vida.

2. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión y los parámetros de precisión pertinentes.

3. Los sistemas de IA de alto riesgo serán resistentes a los errores, fallos e incoherencias que pueden surgir en los propios sistemas o en el entorno donde operan, en particular a causa de su interacción con personas físicas u otros sistemas.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones de redundancia técnica, tales como copias de seguridad o planes de prevención contra fallos.

Los sistemas de IA de alto riesgo que continúan aprendiendo tras su introducción en el mercado o puesta en servicio se desarrollarán de tal modo que los posibles sesgos en la información de salida debidos al uso de esta como datos de entrada en futuras operaciones («bucle de retroalimentación») se subsanen debidamente con las medidas de mitigación oportunas.

4. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso o funcionamiento aprovechando las vulnerabilidades del sistema.

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

Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA figurarán, según corresponda, medidas para prevenir y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («contaminación de datos»), los datos de entrada diseñados para hacer que el modelo cometa un error («ejemplos adversarios») o los defectos en el modelo.

CAPÍTULO 3

OBLIGACIONES DE LOS PROVEEDORES Y USUARIOS DE SISTEMAS DE IA DE ALTO RIESGO Y DE OTRAS PARTES

Artículo 16
Obligaciones de los proveedores de sistemas de IA de alto riesgo

Los proveedores de sistemas de IA de alto riesgo:

a) velarán por que sus sistemas de IA de alto riesgo cumplan los requisitos definidos en el capítulo 2 del presente título;

b) contarán con un sistema de gestión de la calidad que cumpla lo dispuesto en el artículo 17;

c) elaborarán la documentación técnica del sistema de IA de alto riesgo;

d) cuando estén bajo su control, conservarán los archivos de registro que sus sistemas de IA de alto riesgo generen automáticamente;

e) se asegurarán de que los sistemas de IA de alto riesgo sean sometidos al procedimiento de evaluación de la conformidad oportuno antes de su introducción en el mercado o puesta en servicio;

f) cumplirán las obligaciones de registro a que se refiere el artículo 51;

g) adoptarán las medidas correctoras necesarias cuando un sistema de IA de alto riesgo no cumpla los requisitos establecidos en el capítulo 2 del presente título;

h) informarán a las autoridades nacionales competentes del Estado miembro donde hayan comercializado o puesto en servicio el sistema de IA y, en su caso, al organismo notificado de los casos de no conformidad y de las medidas correctoras adoptadas;

i) colocarán el marcado CE en sus sistemas de IA de alto riesgo para indicar que cumplen lo dispuesto en el presente Reglamento, de conformidad con el artículo 49;

j) demostrarán, a solicitud de la autoridad nacional competente, que sus sistemas de IA de alto riesgo cumplen los requisitos establecidos en el capítulo 2 del presente título.

Artículo 17
Sistema de gestión de la calidad

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

a) una estrategia para el cumplimiento reglamentario, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo;

b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo;

c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo y el control y el aseguramiento de la calidad del sistema de IA de alto riesgo;

d) los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que tendrán lugar;

e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla los requisitos establecidos en el capítulo 2 del presente título;

f) los sistemas y procedimientos de gestión de datos, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin;

g) el sistema de gestión de riesgos que se menciona en el artículo 9;

h) el establecimiento, la implantación y el mantenimiento de un sistema de seguimiento posterior a la comercialización con arreglo al artículo 61;

i) los procedimientos asociados a la notificación de incidentes graves y defectos de funcionamiento con arreglo al artículo 62;

j) la gestión de la comunicación con las autoridades nacionales competentes; las autoridades competentes, incluidas las sectoriales, que permiten acceder a datos o facilitan el acceso a ellos; los organismos notificados; otros operadores; los clientes, u otras partes interesadas;

k) los sistemas y procedimientos destinados a llevar un registro de toda la documentación e información pertinente;

l) la gestión de los recursos, incluida la seguridad de las medidas relacionadas con el suministro;

m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado.

2. La inclusión de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor.

3. En el caso de los proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE, se considerará que cumplen la obligación de establecer un sistema de gestión de la calidad cuando cumplan las normas relativas a los sistemas, procedimientos y mecanismos de gobernanza interna que figuran en el artículo 74 de dicha Directiva. En ese contexto, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40 del presente Reglamento.

Artículo 18
Obligación de elaborar documentación técnica

1. Los proveedores de sistemas de IA de alto riesgo elaborarán la documentación técnica mencionada en el artículo 11 con arreglo al anexo IV.

2. En el caso de los proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE, la documentación técnica formará parte de la documentación relativa a los sistemas, procedimientos y mecanismos de gobernanza interna que figuran en el artículo 74 de dicha Directiva.

Artículo 19
Evaluación de la conformidad

1. Los proveedores de sistemas de IA de alto riesgo se asegurarán de que sus sistemas sean sometidos al procedimiento de evaluación de la conformidad oportuno, de conformidad con el artículo 43, antes de su introducción en el mercado o puesta en servicio. Cuando dicha evaluación de la conformidad demuestre que los sistemas de IA cumplen los requisitos establecidos en el capítulo 2 del presente título, sus proveedores elaborarán una declaración UE de conformidad con arreglo al artículo 48 y colocarán el marcado CE de conformidad con arreglo al artículo 49.

2. En el caso de los sistemas de IA de alto riesgo mencionados en el punto 5, letra b), del anexo III, introducidos en el mercado o puestos en servicio por proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE, la evaluación de la conformidad se llevará a cabo como parte del procedimiento a que se refieren los artículos 97 a 101 de la mencionada Directiva.

Artículo 20
Archivos de registro generados automáticamente

1. Los proveedores de sistemas de IA de alto riesgo conservarán los archivos de registro que generen automáticamente sus sistemas de IA de alto riesgo en la medida en que dichos archivos estén bajo su control en virtud de un acuerdo contractual con el usuario o de conformidad con la ley. Conservarán los archivos de registro durante un período de tiempo adecuado en vista de la finalidad prevista del sistema de IA de alto riesgo en cuestión y conforme a las obligaciones jurídicas aplicables con arreglo al Derecho de la Unión o nacional.

2. Los proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE conservarán los archivos de registro que generen automáticamente sus sistemas de IA de alto riesgo como parte de la documentación prevista en el artículo 74 de dicha Directiva.

Artículo 21
Medidas correctoras

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 ponerlo en conformidad, retirarlo del mercado o recuperarlo, según proceda. Informarán de ello a los distribuidores del sistema de IA de alto riesgo en cuestión y, en su caso, al representante autorizado y a los importadores.

Artículo 22
Obligación de información

Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, y el proveedor del sistema sea consciente de dicho riesgo, dicho proveedor informará de inmediato, en particular sobre el incumplimiento y las medidas correctoras adoptadas, a las autoridades nacionales competentes del Estado miembro donde haya comercializado el sistema y, cuando proceda, al organismo notificado que haya expedido el certificado correspondiente al sistema de IA de alto riesgo.

Artículo 23
Cooperación con las autoridades competentes

Los proveedores de sistemas de IA de alto riesgo proporcionarán a las autoridades nacionales competentes que se lo soliciten toda la información y la documentación necesarias para demostrar que sus sistemas de IA de alto riesgo cumplen los requisitos establecidos en el capítulo 2 del presente título, las cuales estarán redactadas en una lengua oficial de la Unión que decidirá el Estado miembro en cuestión. Previa solicitud motivada de una autoridad nacional competente, los proveedores darán a esta acceso a los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo, en la medida en que dichos registros estén bajo su control en virtud de un acuerdo contractual con el usuario o de conformidad con la ley.

Artículo 24
Obligaciones de los fabricantes de productos

Cuando un sistema de IA de alto riesgo asociado a productos a los que se apliquen los actos legislativos mencionados en el anexo II, sección A, se introduzca en el mercado o se ponga en servicio junto al producto fabricado con arreglo a dichos actos legislativos y con el nombre de su fabricante, este será el responsable de que el sistema de IA de que se trate cumpla lo dispuesto en el presente Reglamento y, por lo que al sistema de IA se refiere, tendrá las mismas obligaciones que este Reglamento impone al proveedor.

Artículo 25
Representantes autorizados

1. Antes de comercializar sus sistemas en la Unión, cuando no se pueda identificar a un importador, los proveedores establecidos fuera de la Unión tendrán que designar, mediante un mandato escrito, a un representante autorizado que se encuentre en el territorio de la Unión.

2. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. El mandato permitirá al representante autorizado realizar las tareas siguientes:

   a) conservar una copia de la declaración UE de conformidad y de la documentación técnica de que disponen las autoridades nacionales competentes y las autoridades nacionales a las que se refiere el artículo 63, apartado 7;

   b) proporcionar a una autoridad nacional competente, previa solicitud motivada, toda la información y la documentación necesarias para demostrar que un sistema de IA de alto riesgo cumple los requisitos establecidos en el capítulo 2 del presente título, y en particular en lo que respecta al acceso a los archivos de registro generados automáticamente por ese sistema, en la medida en que dichos archivos estén bajo el control del proveedor en virtud de un acuerdo contractual con el usuario o de conformidad con la ley;

   c) cooperar con las autoridades nacionales competentes, previa solicitud motivada, en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo.

Artículo 26
Obligaciones de los importadores

1. Antes de introducir un sistema de IA de alto riesgo en el mercado, los importadores de dicho sistema se asegurarán de que:

   a) el proveedor de dicho sistema de IA ha llevado a cabo el procedimiento de evaluación de la conformidad oportuno;

   b) el proveedor ha elaborado la documentación técnica de conformidad con el anexo IV;

   c) el sistema lleva el marcado de conformidad pertinente y va acompañado de la documentación y las instrucciones de uso necesarias.

2. Si el importador considera o tiene motivos para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, no podrá introducirlo ese sistema en el mercado hasta que se haya conseguido esa conformidad. Si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 65, apartado 1, el importador informará de ello al proveedor del sistema de IA y a las autoridades de vigilancia del mercado.

3. 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 o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, según proceda.

4. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán, cuando proceda, de que las condiciones de almacenamiento o transporte

no comprometen el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título.

5. Los importadores proporcionarán a las autoridades nacionales competentes, previa solicitud motivada, toda la información y la documentación necesarias para demostrar que un sistema de IA de alto riesgo cumple los requisitos establecidos en el capítulo 2 del presente título, en una lengua que la autoridad nacional competente de que se trate pueda entender con facilitad, y en particular les facilitarán el acceso a los archivos de registro generados automáticamente por ese sistema de IA de alto riesgo, en la medida en que dichos archivos estén bajo el control del proveedor en virtud de un acuerdo contractual con el usuario o de conformidad con la ley. Asimismo, cooperarán con esas autoridades nacionales competentes en todas las acciones que estas emprendan en relación con dicho sistema.

Artículo 27
Obligaciones de los distribuidores

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores verificarán que este lleve el marcado CE de conformidad necesario y vaya acompañado de la documentación y las instrucciones de uso oportunas, y se cerciorarán de que el proveedor y el importador del sistema, según corresponda, hayan cumplido las obligaciones establecidas en el presente Reglamento.

2. Si un distribuidor considera o tiene motivos para considerar que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en el capítulo 2 del presente título, no podrá introducirlo en el mercado hasta que se haya conseguido esa conformidad. Del mismo modo, si el sistema presenta un riesgo en el sentido del artículo 65, apartado 1, el distribuidor informará de ello al proveedor o importador del sistema, según corresponda.

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

4. Los distribuidores que consideren o tengan motivos para considerar que un sistema de IA de alto riesgo que han comercializado no es conforme con los requisitos establecidos en el capítulo 2 del presente título adoptarán las medidas correctoras necesarias para que sea conforme, retirarlo del mercado o recuperarlo, o velarán por que el proveedor, el importador u otro operador pertinente, según proceda, adopte dichas medidas correctoras. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, su distribuidor informará inmediatamente de ello a las autoridades nacionales competentes de los Estados miembros en los que haya comercializado el producto en cuestión y dará detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

5. Previa solicitud motivada de una autoridad nacional competente, los distribuidores de sistemas de IA de alto riesgo proporcionarán a esta toda la información y la documentación necesarias para demostrar que un sistema de IA de alto riesgo cumple los requisitos establecidos en el capítulo 2 del presente título. Asimismo, los distribuidores cooperarán con dicha autoridad nacional competente en cualquier acción que esta emprenda.

Artículo 28

Obligaciones de los distribuidores, los importadores, los usuarios o los terceros

1. Cualquier distribuidor, importador, usuario o tercero será considerado proveedor a los efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor previstas en el artículo 16 en cualquiera de las siguientes circunstancias:

   a) cuando introduzca en el mercado o ponga en servicio un sistema de IA de alto riesgo con su nombre o marca comercial;

   b) cuando modifique la finalidad prevista de un sistema de IA de alto riesgo ya introducido en el mercado o puesto en servicio;

   c) cuando realice una modificación sustancial en el sistema de IA de alto riesgo.

2. Cuando se den las circunstancias mencionadas en el apartado 1, letras b) o c), el proveedor que inicialmente introdujo el sistema de IA de alto riesgo en el mercado o lo puso en servicio dejará de ser considerado proveedor a efectos del presente Reglamento.

Artículo 29

Obligaciones de los usuarios de sistemas de IA de alto riesgo

1. Los usuarios de sistemas de IA de alto riesgo utilizarán dichos sistemas con arreglo a las instrucciones de uso que los acompañen, de acuerdo con los apartados 2 y 5.

2. Las obligaciones previstas en el apartado 1 deben entenderse sin perjuicio de otras obligaciones que el Derecho de la Unión o nacional imponga a los usuarios y no afectarán a su discrecionalidad para organizar sus recursos y actividades con el fin de aplicar las medidas de vigilancia humana que indique el proveedor.

3. Sin perjuicio de lo dispuesto en el apartado 1, el usuario se asegurará de que los datos de entrada sean pertinentes para la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos.

4. Los usuarios vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso. Cuando tengan motivos para considerar que utilizar el sistema de IA conforme a sus instrucciones de uso podría hacer que el sistema de IA presente un riesgo en el sentido del artículo 65, apartado 1, informarán al proveedor o distribuidor y suspenderán el uso del sistema. Del mismo modo, si detectan un incidente grave o un defecto de funcionamiento en el sentido del artículo 62, informarán al proveedor o distribuidor e interrumpirán el uso del sistema de IA. En el caso de que el usuario no consiga contactar con el proveedor, el artículo 62 se aplicará *mutatis mutandis*.

   En el caso de los usuarios que sean entidades de crédito reguladas por la Directiva 2013/36/UE, se considerará que cumplen la obligación de vigilancia establecida en el párrafo primero cuando cumplan las normas relativas a los sistemas, procedimientos y mecanismos de gobernanza interna que figuran en el artículo 74 de dicha Directiva.

5. Los usuarios de sistemas de IA de alto riesgo conservarán los archivos de registro que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control. Conservarán los archivos durante un período de tiempo adecuado en vista de la finalidad prevista del sistema de IA de alto riesgo

de que se trate y conforme a las obligaciones jurídicas aplicables con arreglo al Derecho de la Unión o nacional.

En el caso de los usuarios que sean entidades de crédito reguladas por la Directiva 2013/36/UE, los archivos de registro formarán parte de la documentación relativa a los sistemas, procedimientos y mecanismos de gobernanza interna que figuran en el artículo 74 de dicha Directiva.

6. Los usuarios de sistemas de IA de alto riesgo utilizarán la información facilitada conforme al artículo 13 para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos que les imponen el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, cuando corresponda.

CAPÍTULO 4

AUTORIDADES NOTIFICANTES Y ORGANISMOS NOTIFICADOS

Artículo 30
Autoridades notificantes

1. Cada Estado miembro nombrará o constituirá una autoridad notificante que será responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su seguimiento.

2. Los Estados miembros podrán designar un organismo nacional de acreditación, según lo contemplado en el Reglamento (CE) n.º 765/2008, como autoridad notificante.

3. Las autoridades notificantes se constituirán, organizarán y operarán de forma que no surjan conflictos de interés con los organismos de evaluación de la conformidad y que se garantice la imparcialidad y objetividad de sus actividades.

4. 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.

5. Las autoridades notificantes no ofrecerán ni ejercerán ninguna actividad que efectúen los organismos de evaluación de la conformidad ni ningún servicio de consultas de carácter comercial o competitivo.

6. Las autoridades notificantes preservarán la confidencialidad de la información obtenida.

7. Las autoridades notificantes dispondrán de suficiente personal competente para efectuar adecuadamente sus tareas.

8. Las autoridades notificantes velarán por que las evaluaciones de la conformidad se lleven a cabo de forma proporcionada, evitando cargas innecesarias para los proveedores, y por que los organismos notificados desempeñen sus actividades teniendo debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura y el grado de complejidad del sistema de IA en cuestión.

Artículo 31

Solicitud de notificación por parte de un organismo de evaluación de la conformidad

1. Los organismos de evaluación de la conformidad presentarán una solicitud de notificación ante 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 las tecnologías de inteligencia artificial en relación con las cuales 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 en virtud de cualquier otra legislación de armonización de la Unión.

3. Si el organismo de evaluación de la conformidad de que se trate no puede facilitar un certificado de acreditación, entregará a la autoridad notificante todas las pruebas documentales necesarias para verificar, reconocer y supervisar regularmente que cumple los requisitos establecidos en el artículo 33. En lo que respecta a los organismos notificados designados de conformidad con cualquier otra legislación de armonización de la Unión, todos los documentos y certificados vinculados a dichas designaciones podrán utilizarse para apoyar su procedimiento de designación en virtud del presente Reglamento, según proceda.

Artículo 32

Procedimiento de notificación

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

2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros mediante la herramienta de notificación electrónica desarrollada y gestionada por la Comisión.

3. La notificación incluirá información pormenorizada de las actividades de evaluación de la conformidad, el módulo o los módulos de evaluación de la conformidad y las tecnologías de inteligencia artificial afectadas.

4. El organismo de evaluación de la conformidad en cuestión únicamente podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no formulan ninguna objeción en el plazo de un mes tras la notificación.

5. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros todo cambio posterior de la notificación que resulte pertinente.

Artículo 33

Organismos notificados

1. Los organismos notificados verificarán la conformidad de los sistemas de IA de alto riesgo siguiendo los procedimientos de evaluación de la conformidad contemplados en el artículo 43.

2. Los organismos notificados satisfarán los requisitos organizativos, así como los de gestión de la calidad, recursos y procesos, necesarios para el desempeño de sus funciones.

3. La estructura organizativa, la distribución de las responsabilidades, la línea jerárquica y el funcionamiento de los organismos notificados serán tales que ofrezcan confianza en el desempeño y en los resultados de las actividades de evaluación de la conformidad que realicen los organismos notificados.

4. Los organismos notificados serán independientes del proveedor de un sistema de IA de alto riesgo en relación con el cual lleven a cabo actividades de evaluación de la conformidad. Los organismos notificados serán independientes de cualquier otro operador con un interés económico en el sistema de IA de alto riesgo que se evalúe, así como de cualquier competidor del proveedor.

5. Los organismos notificados estarán organizados y gestionados de modo que se garantice la independencia, objetividad e imparcialidad de sus actividades. Los organismos notificados documentarán e implantarán una estructura y procedimientos que garanticen la imparcialidad y permitan promover y aplicar los principios de imparcialidad aplicables en toda su organización y a todo su personal y actividades de evaluación.

6. Los organismos notificados se dotarán de procedimientos documentados que garanticen que su personal, sus comités, sus filiales, sus subcontratistas y todos sus organismos asociados o personal de organismos externos respeten la confidencialidad de la información de la que tengan conocimiento en el ejercicio de las actividades de evaluación de la conformidad, excepto en aquellos casos en que la ley exija la divulgación de tal información. El personal de los organismos notificados estará sujeto al secreto profesional en lo que respecta a toda la información obtenida en el ejercicio de las tareas encomendadas en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que desarrollen sus actividades.

7. Los organismos notificados contarán con procedimientos para desempeñar sus actividades que tengan debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura y el grado de complejidad del sistema de IA de que se trate.

8. Los organismos notificados suscribirán un seguro de responsabilidad adecuado para sus actividades de evaluación de la conformidad, salvo que dicha responsabilidad se halle cubierta por el Estado miembro correspondiente con arreglo a la legislación nacional o que dicho Estado miembro sea directamente responsable de la evaluación de la conformidad.

9. Los organismos notificados serán capaces de llevar a cabo todas las tareas que les competan con arreglo al presente Reglamento con el máximo grado de integridad profesional y la competencia técnica necesaria en el ámbito específico, tanto si dichas tareas las efectúan los propios organismos notificados como si se realizan en su nombre y bajo su responsabilidad.

10. Los organismos notificados contarán con competencias internas suficientes para poder evaluar de manera eficaz las tareas que lleven a cabo agentes externos en su nombre. Para ello, en todo momento y para cada procedimiento de evaluación de la conformidad y cada tipo de sistema de IA de alto riesgo para los que haya sido designado, el organismo notificado dispondrá permanentemente de suficiente

personal administrativo, técnico y científico que posea experiencia y conocimientos relativos a las tecnologías de inteligencia artificial, datos y computación de datos pertinentes y a los requisitos establecidos en el capítulo 2 del presente título.

11. Los organismos notificados participarán en las actividades de coordinación según lo previsto en el artículo 38. Asimismo, tomarán parte directamente o mediante representación en organizaciones europeas de normalización, o se asegurarán de mantenerse al corriente de la situación actualizada de las normas correspondientes.

12. Los organismos notificados pondrán a disposición de la autoridad notificante mencionada en el artículo 30, y les presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, que permita a la autoridad notificante ejercer sus funciones de evaluación, designación, notificación, seguimiento y vigilancia y facilitar la evaluación descrita en el presente capítulo.

Artículo 34
Filiales y subcontratación de organismos notificados

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 cumplan 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 los subcontratistas o las filiales con independencia del lugar de establecimiento de estos.

3. Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del proveedor.

4. Los organismos notificados mantendrán a disposición de la autoridad notificante los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial, así como el trabajo que estos realicen con arreglo al presente Reglamento.

Artículo 35
Números de identificación y listas de organismos notificados designados de conformidad con el presente Reglamento

1. La Comisión asignará un número de identificación a cada organismo notificado. Asignará un solo número incluso cuando un organismo sea notificado con arreglo a varios actos de la Unión.

2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, junto con los números de identificación que les hayan sido asignados y las actividades para las que hayan sido notificados. La Comisión se asegurará de que la lista se mantenga actualizada.

Artículo 36
Cambios en las notificaciones

1. Si una autoridad notificante sospecha o es informada de que un organismo notificado ya no cumple los requisitos establecidos en el artículo 33 o no está cumpliendo sus obligaciones, dicha autoridad investigará sin demora el asunto con la máxima

diligencia. En ese contexto, informará al organismo notificado de que se trate acerca de las objeciones formuladas y le ofrecerá la posibilidad de exponer sus puntos de vista. Si la autoridad notificante llega a la conclusión de que el organismo notificado sometido a investigación ya no cumple los requisitos establecidos en el artículo 33 o no está cumpliendo sus obligaciones, dicha autoridad restringirá, suspenderá o retirará la notificación, según el caso, dependiendo de la gravedad del incumplimiento. Asimismo, informará de ello inmediatamente a la Comisión y a los demás Estados miembros.

2. En caso de restricción, suspensión o retirada de la notificación, o si el organismo notificado ha cesado su actividad, la autoridad notificante adoptará las medidas oportunas para asegurarse de que los expedientes de dicho organismo notificado sean asumidos por otro organismo notificado o se pongan a disposición de las autoridades notificantes responsables cuando estas los soliciten.

Artículo 37
Impugnación de la competencia de los organismos notificados

1. La Comisión investigará, cuando sea necesario, todos los casos en los que existan razones para dudar de que un organismo notificado cumpla los requisitos establecidos en el artículo 33.

2. La autoridad notificante facilitará a la Comisión, a petición de esta, toda la información pertinente relativa a la notificación del organismo notificado que corresponda.

3. La Comisión garantizará el tratamiento confidencial de toda la información de esa naturaleza recabada en el transcurso de sus investigaciones de conformidad con el presente artículo.

4. Cuando la Comisión compruebe que un organismo notificado no cumple o ha dejado de cumplir los requisitos establecidos en el artículo 33, adoptará una decisión motivada por la que solicitará al Estado miembro notificante que adopte las medidas correctoras necesarias, entre ellas la retirada de la notificación cuando sea necesario. 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 se asegurará de que se instaure y se gestione convenientemente, en relación con los ámbitos cubiertos por el presente Reglamento, una adecuada coordinación y cooperación entre los organismos notificados activos en los procedimientos de evaluación de la conformidad de los sistemas de IA en virtud del presente Reglamento, en forma de grupo sectorial de organismos notificados.

2. Los Estados miembros se asegurarán de que los organismos por ellos notificados participan en el trabajo de este grupo directamente o por medio de representantes designados.

Artículo 39
Organismos de evaluación de la conformidad de terceros países

Los organismos de evaluación de la conformidad establecidos conforme al Derecho de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados para desempeñar las actividades de los organismos notificados con arreglo al presente Reglamento.

CAPÍTULO 5

NORMAS, EVALUACIÓN DE LA CONFORMIDAD, CERTIFICADOS, REGISTRO

Artículo 40
Normas armonizadas

Se presumirá que los sistemas de IA de alto riesgo que sean conformes con normas armonizadas, o partes de estas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* son conformes con los requisitos establecidos en el capítulo 2 del presente título en la medida en que dichas normas prevean estos requisitos.

Artículo 41
Especificaciones comunes

1. Cuando las normas armonizadas mencionadas en el artículo 40 no existan o cuando la Comisión considere que las normas armonizadas pertinentes son insuficientes o que es necesario abordar cuestiones específicas relacionadas con la seguridad o con los derechos fundamentales, la Comisión, mediante actos de ejecución, podrá adoptar especificaciones comunes en relación con los requisitos establecidos en el capítulo 2 del presente título. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

2. Al elaborar las especificaciones comunes a que se refiere el apartado 1, la Comisión recabará los puntos de vista de los organismos o grupos de expertos pertinentes establecidos de conformidad con el Derecho de la Unión aplicable a nivel sectorial.

3. Se presumirá que los sistemas de IA de alto riesgo que sean conformes con las especificaciones comunes mencionadas en el apartado 1 son conformes con los requisitos establecidos en el capítulo 2 del presente título, en la medida en que dichas especificaciones comunes prevean estos requisitos.

4. Cuando los proveedores no cumplan las especificaciones comunes mencionadas en el apartado 1, justificarán debidamente que han adoptado soluciones técnicas como mínimo equivalentes a aquellas.

Artículo 42
Presunción de conformidad con determinados requisitos

1. Teniendo en cuenta su finalidad prevista, se presumirá que los sistemas de IA de alto riesgo que hayan sido entrenados y probados con datos relativos al entorno geográfico, conductual y funcional específico en el que esté previsto su uso cumplan el requisito establecido en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo que hayan sido certificados o para los que se haya expedido una declaración de conformidad con arreglo a un esquema de ciberseguridad en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo

y del Consejo[63] 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 estos, prevean estos 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 el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título por parte de un sistema de IA de alto riesgo, el proveedor haya aplicado normas armonizadas a que se refiere el artículo 40, o bien, en su caso, especificaciones comunes a que se refiere el artículo 41, el proveedor se atendrá a uno de los procedimientos siguientes:

   a) el procedimiento de evaluación de la conformidad fundamentado en un control interno mencionado en el anexo VI;

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

   Cuando, al demostrar el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título por parte de un sistema de IA de alto riesgo, el proveedor no haya aplicado las normas armonizadas a que se refiere el artículo 40 o solo las haya aplicado parcialmente, o cuando no existan tales normas armonizadas y no se disponga de especificaciones comunes a que se refiere el artículo 41, el proveedor se atendrá al procedimiento de evaluación de la conformidad establecido en el anexo VII.

   A efectos del procedimiento de evaluación de la conformidad establecido en el anexo VII, el proveedor podrá escoger cualquiera de los organismos notificados. No obstante, cuando se prevea la puesta en servicio del sistema por parte de las autoridades encargadas de la aplicación de la ley, las autoridades de inmigración y asilo, así como las instituciones, los organismos o las agencias de la UE, la autoridad de vigilancia del mercado mencionada en el artículo 63, apartado 5 o 6, según proceda, actuará como organismo notificado.

2. En el caso de los sistemas de IA de alto riesgo mencionados en los puntos 2 a 8 del anexo III, los proveedores se atendrán al procedimiento de evaluación de la conformidad fundamentado en un control interno a que se refiere el anexo VI, que no contempla la participación de un organismo notificado. En el caso de los sistemas de IA de alto riesgo mencionados en el punto 5, letra b), del anexo III, introducidos en el mercado o puestos en servicio por entidades de crédito reguladas por la Directiva 2013/36/UE, la evaluación de la conformidad se llevará a cabo como parte del procedimiento a que se refieren los artículos 97 a 101 de la mencionada Directiva.

[63] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad) (DO L 151 de 7.6.2019, p. 1).

3. En el caso de los sistemas de IA de alto riesgo a los que sean de aplicación los actos legislativos enumerados en el anexo II, sección A, el proveedor se atendrá a la evaluación de la conformidad pertinente exigida por dichos actos legislativos. 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. Asimismo, se aplicarán los puntos 4.3, 4.4, 4.5 y 4.6, párrafo quinto, del anexo VII.

   A efectos de dicha evaluación, los organismos notificados que hayan sido notificados con arreglo a dichos actos legislativos dispondrán de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos dispuestos en el artículo 33, apartados 4, 9 y 10, en el contexto del procedimiento de notificación contemplado en dichos actos legislativos.

   Cuando los actos legislativos enumerados en el anexo II, sección A, permitan al fabricante del producto prescindir de una evaluación de conformidad realizada por terceros, a condición de que el fabricante haya aplicado todas las normas armonizadas que cubran todos los requisitos pertinentes, dicho fabricante solamente podrá recurrir a esta opción si también ha aplicado normas armonizadas, o, en su caso, 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 se someterán a un nuevo procedimiento de evaluación de la conformidad siempre que se modifiquen de manera sustancial, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el usuario actual.

   En el caso de los sistemas de IA de alto riesgo que continúen aprendiendo tras su introducción en el mercado o su puesta en servicio, los cambios en el sistema de IA de alto riesgo y su funcionamiento que hayan sido predeterminados por el proveedor en el momento de la evaluación inicial de la conformidad y figuren incluidos en la información recogida en la documentación técnica mencionada en el punto 2, letra f), del anexo IV no constituirán modificaciones sustanciales.

5. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de actualizar los anexos VI y VII para introducir elementos de los procedimientos de evaluación de la conformidad que resulten necesarios a la luz del progreso técnico.

6. Se otorgan a la Comisión los poderes para adoptar actos delegados que modifiquen los apartados 1 y 2 a fin de someter a los sistemas de IA de alto riesgo mencionados en los puntos 2 a 8 del anexo III al procedimiento de evaluación de la conformidad a que se refiere el anexo VII o a partes de este. La Comisión adoptará dichos actos delegados teniendo en cuenta la eficacia del procedimiento de evaluación de la conformidad fundamentado en un control interno contemplado en el anexo VI para prevenir o reducir al mínimo los riesgos para la salud, la seguridad y la protección de los derechos fundamentales que plantean estos sistemas, así como la disponibilidad de capacidades y recursos adecuados por parte de los organismos notificados.

Artículo 44
Certificados

1. Los certificados expedidos por organismos notificados con arreglo al anexo VII se redactarán en una lengua oficial de la Unión determinada por el Estado miembro en el que esté establecido el organismo notificado o en una lengua oficial de la Unión que resulte aceptable para este último.

2. Los certificados serán válidos para el período que indican, que no excederá de cinco años. A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos renovables no superiores a cinco años, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables.

3. Si un organismo notificado observa que un sistema de IA ya no cumple los requisitos establecidos en el capítulo 2 del presente título, suspenderá o retirará, teniendo en cuenta el principio de proporcionalidad, el certificado expedido o le impondrá restricciones, a menos que se garantice el cumplimiento de dichos requisitos mediante medidas correctoras adecuadas adoptadas por el proveedor del sistema en un plazo adecuado determinado por el organismo notificado. El organismo notificado motivará su decisión.

Artículo 45
Recurso frente a las decisiones de los organismos notificados

Los Estados miembros velarán por que exista un procedimiento de recurso contra las decisiones de los organismos notificados a disposición de las partes que tengan un interés legítimo en dichas decisiones.

Artículo 46
Obligaciones de información de los organismos notificados

1. Los organismos notificados informarán a la autoridad notificante:

   a) de cualquier certificado de la Unión de evaluación de la documentación técnica, cualquier suplemento a dichos certificados y las aprobaciones de sistemas de gestión de la calidad expedidos con arreglo a las condiciones establecidas en el anexo VII;

   b) de cualquier denegación, restricción, suspensión o retirada de un certificado de la Unión de evaluación de la documentación técnica o de una aprobación de un sistema de gestión de la calidad expedidos con arreglo a las condiciones establecidas en el anexo VII;

   c) de cualquier circunstancia que afecte al ámbito o a las condiciones de notificación;

   d) de toda solicitud de información sobre las actividades de evaluación de la conformidad que hayan recibido de las autoridades de vigilancia del mercado;

   e) previa solicitud, de las actividades de evaluación de la conformidad realizadas dentro del ámbito de su notificación y de cualquier otra actividad realizada, con inclusión de las actividades transfronterizas y las subcontrataciones.

2. Cada organismo notificado informará a los demás organismos notificados:

a) de las aprobaciones de sistemas de gestión de la calidad que haya rechazado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de calidad que haya expedido;

b) de los certificados de evaluación de la documentación técnica de la UE o los suplementos a dichos certificados que haya rechazado, retirado, suspendido o restringido de cualquier otro modo, y, previa solicitud, de los certificados o los suplementos a estos que haya expedido.

3. Cada organismo notificado proporcionará a los demás organismos notificados que realicen actividades de evaluación de la conformidad similares y relativas a las mismas tecnologías de inteligencia artificial información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de las evaluaciones de la conformidad.

Artículo 47
Exención del procedimiento de evaluación de la conformidad

1. No obstante lo dispuesto en el artículo 43, 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 razones excepcionales de seguridad pública o con el fin de proteger la vida y la salud de las personas, el medio ambiente y activos fundamentales de las industrias e infraestructuras. Dicha autorización se concederá para un período limitado, mientras se lleven a cabo los procedimientos de evaluación de la conformidad necesarios, y finalizará una vez concluidos dichos procedimientos. La conclusión de los procedimientos en cuestión se alcanzará sin demora indebida.

2. La autorización a que se refiere el apartado 1 solo 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 establecidos en el 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 de conformidad con el apartado 1.

3. Si, en el plazo de quince días naturales tras la recepción de la información indicada en el apartado 2, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una autorización expedida por una autoridad de vigilancia del mercado de un Estado miembro con arreglo al apartado 1, la autorización se considerará justificada.

4. Si, en el plazo de quince días naturales tras la recepción de la notificación a que se refiere el apartado 2, un Estado miembro formula objeciones contra una autorización expedida por una autoridad de vigilancia del mercado de otro Estado miembro, o si la Comisión considera que la autorización vulnera el Derecho de la Unión o que la conclusión de los Estados miembros relativa al cumplimiento del sistema a que se refiere el apartado 2 es infundada, la Comisión celebrará consultas con el Estado miembro pertinente sin demora; se consultará al operador u operadores de que se trate y se les ofrecerá la posibilidad de exponer sus puntos de vista. En vista de todo ello, la Comisión decidirá si la autorización está justificada o no. La Comisión enviará su decisión al Estado miembro afectado y al operador u operadores pertinentes.

5. Si la autorización no se considera justificada, la autoridad de vigilancia del mercado del Estado miembro de que se trate la retirará.

6. No obstante lo dispuesto en los apartados 1 a 5, en el caso de los sistemas de IA de alto riesgo destinados a utilizarse como componentes de seguridad de dispositivos o que en sí mismos son dispositivos, cubiertos por el Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746, el artículo 59 del Reglamento (UE) 2017/745 y el artículo 54 del Reglamento (UE) 2017/746 serán igualmente de aplicación con respecto a la exención de la evaluación de la conformidad relativa al cumplimiento de los requisitos establecidos en el capítulo 2 del presente título.

Artículo 48
Declaración UE de conformidad

1. El proveedor redactará una declaración UE de conformidad para cada sistema de IA y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años después de la introducción del sistema de IA en el mercado o su puesta en servicio. En la declaración UE de conformidad se identificará el sistema de IA para el que ha sido redactada. Se facilitará una copia de la declaración UE de conformidad a las autoridades nacionales competentes pertinentes que lo soliciten.

2. En la declaración UE de conformidad constará que el sistema de IA de alto riesgo de que se trate cumple los requisitos especificados en el capítulo 2 del presente título. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a la lengua o lenguas oficiales de la Unión que requiera el Estado o Estados miembros en que se comercialice el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sometidos a otra legislación de armonización de la Unión que también requiera una declaración UE de conformidad, se establecerá una única declaración UE de conformidad relativa a todas las legislaciones de la Unión aplicables al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para identificar la legislación de armonización de la Unión a la que la propia declaración se refiera.

4. Al redactar 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.

5. Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73 al objeto de actualizar el contenido de la declaración UE de conformidad dispuesta en el anexo V con el fin de introducir elementos que resulten necesarios a la luz del progreso técnico.

Artículo 49
Marcado CE de conformidad

1. El marcado CE se colocará de manera visible, legible e indeleble en los sistemas de IA de alto riesgo. Cuando esto 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 los documentos adjuntos, según proceda.

2. El marcado CE a que se refiere el apartado 1 del presente artículo estará sujeto a los principios generales contemplados en el artículo 30 del Reglamento (CE) n.º 765/2008.

3. En su caso, 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 figurará también en todo el material publicitario en el que se mencione que el sistema de IA de alto riesgo cumple los requisitos de marcado CE.

Artículo 50
Conservación de los documentos

Durante un período que finalizará diez años después de la introducción del sistema de IA en el mercado o su puesta en servicio, el proveedor mantendrá a disposición de las autoridades nacionales competentes:

a) la documentación técnica a que se refiere el artículo 11;

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

c) la documentación relativa a los cambios aprobados por los organismos notificados, si procede;

d) las decisiones y otros documentos expedidos por los organismos notificados, si procede;

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

Artículo 51
Inscripción en el registro

Antes de la introducción en el mercado o la puesta en servicio de un sistema de IA de alto riesgo contemplado en el artículo 6, apartado 2, el proveedor o, en su caso, el representante autorizado registrará dicho sistema en la base de datos de la UE a que se refiere el artículo 60.

TÍTULO IV

OBLIGACIONES DE TRANSPARENCIA PARA DETERMINADOS SISTEMAS DE IA

Artículo 52
Obligaciones de transparencia para determinados sistemas de IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA, excepto en las situaciones en las que esto resulte evidente debido a las circunstancias y al contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por la ley para fines de detección, prevención, investigación o enjuiciamiento de infracciones penales, salvo que estos sistemas estén a disposición del público para denunciar una infracción penal.

2. Los usuarios de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él. Esta obligación no se aplicará a los sistemas de IA utilizados

para la categorización biométrica autorizados por la ley para fines de detección, prevención e investigación de infracciones penales.

3. Los usuarios de un sistema de IA que genere o manipule contenido de imagen, sonido o vídeo que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos (ultrafalsificación), harán público que el contenido ha sido generado de forma artificial o manipulado.

   No obstante, el primer párrafo no se aplicará cuando el uso esté legalmente por la ley para fines de detección, prevención, investigación y enjuiciamiento de infracciones penales o resulte necesario para el ejercicio del derecho a la libertad de expresión y el derecho a la libertad de las artes y de las ciencias, garantizados por la Carta de los Derechos Fundamentales de la Unión Europea y supeditados a unas garantías adecuadas para los derechos y libertades de terceros.

4. Los apartados 1, 2 y 3 no afectarán a los requisitos y obligaciones dispuestos en el título III del presente Reglamento.

TÍTULO V

MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 53
Espacios controlados de pruebas para la IA

1. Los espacios controlados de pruebas para la IA establecidos por las autoridades competentes de uno o varios Estados miembros o por el Supervisor Europeo de Protección de Datos proporcionarán un entorno controlado que facilite el desarrollo, la prueba y la validación de sistemas innovadores de IA durante un período limitado antes de su introducción en el mercado o su puesta en servicio, en virtud de un plan específico. Esto se llevará a cabo bajo la supervisión y la orientación directas de las autoridades competentes con el fin de garantizar el cumplimiento de los requisitos establecidos en el presente Reglamento y, en su caso, en otras legislaciones de la Unión y de los Estados miembros supervisadas en el marco del espacio controlado de pruebas.

2. Los Estados miembros velarán por que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o respalden el acceso a los datos, las autoridades nacionales de protección de datos y las demás autoridades nacionales estén ligadas al funcionamiento del espacio controlado de pruebas para la IA.

3. Los espacios controlados de pruebas para la IA no afectarán a las facultades de supervisión y correctoras de las autoridades competentes. Cualquier riesgo significativo para la salud, la seguridad y los derechos fundamentales detectado durante el proceso de desarrollo y prueba de estos sistemas implicará la mitigación inmediata y, en su defecto, la suspensión del proceso de desarrollo y prueba hasta que se produzca dicha mitigación.

4. Los participantes en los espacios controlados de pruebas para la IA responderán de cualquier perjuicio infligido a terceros como resultado de la experimentación

realizada en el espacio controlado de pruebas, con arreglo a la legislación aplicable de la Unión y de los Estados miembros en materia de responsabilidad.

5. Las autoridades competentes de los Estados miembros que hayan establecido espacios controlados de pruebas para la IA coordinarán sus actividades y cooperarán en el marco del Comité Europeo de Inteligencia Artificial. Presentarán informes anuales al Comité y a la Comisión sobre los resultados de la aplicación de dicho esquema, que incluirán buenas prácticas, enseñanzas extraídas y recomendaciones acerca de su configuración, y, en su caso, sobre la aplicación del presente Reglamento y otra legislación de la Unión supervisada en el marco del espacio controlado de pruebas.

6. Las modalidades y condiciones de funcionamiento de los espacios controlados de pruebas para la IA, incluidos los criterios de admisibilidad y el procedimiento de solicitud, selección, participación y salida del espacio controlado de pruebas, así como los derechos y obligaciones de los participantes, se determinarán en actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

Artículo 54

Tratamiento ulterior de datos personales para el desarrollo de determinados sistemas de IA en aras del interés público en el espacio controlado de pruebas para la IA

1. En el espacio controlado de pruebas para la IA, se tratarán datos personales legalmente recopilados con otros fines con el objetivo de desarrollar y probar determinados sistemas innovadores de IA en el espacio controlado de pruebas, con arreglo a las siguientes condiciones:

   a) que los sistemas innovadores de IA se desarrollen para proteger un interés público esencial en uno o varios de los siguientes ámbitos:

      i) la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, bajo el control y responsabilidad de las autoridades competentes. El tratamiento se basará en el Derecho de la Unión o del Estado miembro;

      ii) la seguridad y la salud públicas, incluida la prevención, el control y el tratamiento de enfermedades;

      iii) un elevado nivel de protección y mejora de la calidad del medio ambiente;

   b) que los datos tratados resulten necesarios para cumplir uno o varios de los requisitos contemplados en el título III, capítulo 2, cuando dichos requisitos no puedan cumplirse debidamente mediante el tratamiento de datos anonimizados, sintéticos u otro tipo de datos no personales;

   c) que existan mecanismos de seguimiento eficaces para detectar si pueden producirse riesgos elevados para los derechos fundamentales o para los interesados durante la experimentación en el espacio controlado de pruebas, así como mecanismos de respuesta para mitigar sin demora dichos riesgos y, en su caso, detener el tratamiento;

   d) que todos los datos personales que se traten en el contexto del espacio controlado de pruebas se encuentren en un entorno de tratamiento de datos

funcionalmente separado, aislado y protegido, bajo el control de los participantes y únicamente accesible para las personas autorizadas;

e) que los datos personales tratados no se transmitan o transfieran a terceros ni sean accesibles de ningún otro modo para ellos;

f) que el tratamiento de datos personales en el contexto del espacio controlado de pruebas no dé lugar a medidas o decisiones que afecten a los interesados;

g) que los datos personales tratados en el contexto del espacio controlado de pruebas se eliminen una vez concluida la participación en dicho espacio o cuando los datos personales lleguen al final de su período de conservación;

h) que los archivos de registro del tratamiento de datos personales en el contexto del espacio controlado de pruebas se conserven mientras dure la participación en el espacio controlado de pruebas y durante un año después de su conclusión, únicamente con el fin de cumplir con las obligaciones en materia de rendición de cuentas y documentación que impone el presente artículo u otra legislación de la Unión o de los Estados miembros que resulte de aplicación, y solo durante el tiempo necesario para ello;

i) que se conserve una descripción completa y detallada del proceso y la justificación del entrenamiento, la prueba y la validación del sistema de IA junto con los resultados del proceso de prueba como parte de la documentación técnica a que se refiere el anexo IV;

j) que se publique una breve síntesis del proyecto de IA desarrollado en el espacio controlado de pruebas, junto con sus objetivos y resultados previstos, en el sitio web de las autoridades competentes.

2. El apartado 1 debe entenderse sin perjuicio de la legislación de la Unión o los Estados miembros que proscriba el tratamiento con fines distintos de los explícitamente mencionados en dicha legislación.

Artículo 55
Medidas dirigidas a proveedores y usuarios a pequeña escala

1. Los Estados miembros adoptarán las medidas siguientes:

a) proporcionar a los proveedores a pequeña escala y a las empresas emergentes un acceso prioritario a los espacios controlados de pruebas para la IA, siempre y cuando cumplan los requisitos de admisibilidad;

b) organizar actividades de sensibilización específicas acerca de la aplicación del presente Reglamento, adaptadas a las necesidades de los proveedores y usuarios a pequeña escala;

c) establecer, cuando proceda, un canal específico para la comunicación con los proveedores y usuarios a pequeña escala, así como con otros agentes innovadores, con objeto de formular orientaciones y responder a las dudas planteadas acerca de la aplicación del presente Reglamento.

2. Se tendrán en cuenta los intereses y necesidades específicos de los proveedores a pequeña escala a la hora de fijar las tasas para la evaluación de la conformidad en virtud del artículo 43, y reducir dichas tasas en proporción a su tamaño y al del mercado.

TÍTULO VI

GOBERNANZA

CAPÍTULO 1

COMITÉ EUROPEO DE INTELIGENCIA ARTIFICIAL

Artículo 56
Constitución del Comité Europeo de Inteligencia Artificial

1. Se establece un «Comité Europeo de Inteligencia Artificial» (el «Comité»).
2. El Comité ofrecerá asesoramiento y asistencia a la Comisión a fin de:
   a) contribuir a la cooperación efectiva de las autoridades nacionales de supervisión y la Comisión con respecto a las materias reguladas por el presente Reglamento;
   b) coordinar y contribuir a las orientaciones y los análisis de la Comisión y las autoridades nacionales de supervisión y otras autoridades competentes sobre problemas emergentes en el mercado interior con respecto a las materias reguladas por el presente Reglamento;
   c) asistir a las autoridades nacionales de supervisión y a la Comisión para garantizar la aplicación coherente del presente Reglamento.

Artículo 57
Estructura del Comité

1. El Comité estará compuesto por las autoridades nacionales de supervisión, que estarán representadas por el jefe de dicha autoridad o un funcionario de alto nivel equivalente, y el Supervisor Europeo de Protección de Datos. Se podrá invitar a otras autoridades nacionales a las reuniones, cuando los temas tratados sean de relevancia para ellas.
2. El Comité adoptará su propio reglamento interno por mayoría simple de los miembros que lo componen, tras el dictamen conforme de la Comisión. En el reglamento interno se recogerán asimismo los aspectos operativos relacionados con la ejecución de las funciones del Comité previstas en el artículo 58. El Comité podrá establecer subgrupos, según proceda, para examinar cuestiones específicas.
3. El Comité estará presidido por la Comisión. La Comisión convocará las reuniones y elaborará el orden del día de conformidad con las funciones del Comité en virtud del presente Reglamento y con su reglamento interno. La Comisión prestará apoyo administrativo y analítico a las actividades del Comité en virtud del presente Reglamento.
4. El Comité podrá invitar a expertos y observadores externos a que asistan a sus reuniones y podrá realizar intercambios con terceros interesados para orientar sus actividades, en la medida en que se considere apropiado. Para ello, la Comisión podrá facilitar intercambios entre el Comité y otros organismos, oficinas, agencias y grupos consultivos de la Unión.

Artículo 58
Funciones del Comité

Cuando preste asesoramiento y asistencia a la Comisión en el contexto del artículo 56, apartado 2, el Comité, en particular:

a) recopilará y compartirá conocimientos técnicos y buenas prácticas entre los Estados miembros;

b) contribuirá a uniformizar las prácticas administrativas en los Estados miembros, incluidas las relativas al funcionamiento de los espacios controlados de pruebas a que se refiere el artículo 53;

c) emitirá dictámenes, recomendaciones o contribuciones por escrito sobre cuestiones relacionadas con la aplicación del presente Reglamento, en particular:

   i) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el título III, capítulo 2;

   ii) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41;

   iii) sobre la preparación de documentos de orientación, incluidas las directrices relativas a la fijación de multas administrativas a que se refiere el artículo 71.

CAPÍTULO 2

AUTORIDADES NACIONALES COMPETENTES

Artículo 59
Designación de autoridades nacionales competentes

1. Cada Estado miembro establecerá o designará autoridades nacionales competentes con el fin de garantizar la aplicación y ejecución del presente Reglamento. Las autoridades nacionales competentes se organizarán de manera que se preserve la objetividad e imparcialidad de sus actividades y funciones.

2. Cada Estado miembro designará una autoridad nacional de supervisión entre las autoridades nacionales competentes. La autoridad nacional de supervisión actuará como autoridad notificante y como autoridad de vigilancia del mercado, salvo que un Estado miembro tenga razones organizativas o administrativas para designar más de una autoridad.

3. Los Estados miembros informarán a la Comisión de su designación o designaciones y, en su caso, de los motivos para designar más de una autoridad.

4. Los Estados miembros garantizarán que las autoridades nacionales competentes dispongan de recursos financieros y humanos adecuados para el desempeño de sus funciones con arreglo al presente Reglamento. En concreto, las autoridades nacionales competentes dispondrán permanentemente de suficiente personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo de las tecnologías de inteligencia artificial, datos y computación de datos; los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes.

5. Los Estados miembros presentarán a la Comisión un informe anual acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes,

que incluirá una evaluación de su idoneidad. La Comisión transmitirá dicha información al Comité para su debate y la formulación de posibles recomendaciones.

6. La Comisión facilitará el intercambio de experiencias entre las autoridades nacionales competentes.

7. Las autoridades nacionales competentes podrán proporcionar orientaciones y asesoramiento acerca de la aplicación del presente Reglamento, incluso a proveedores a pequeña escala. Siempre que una autoridad nacional competente pretenda proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otra legislación de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dicha legislación de la Unión, según proceda. Asimismo, los Estados miembros podrán establecer un punto de contacto central para la comunicación con los operadores.

8. 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 SISTEMAS DE IA DE ALTO RIESGO INDEPENDIENTES

Artículo 60

Base de datos de la UE para sistemas de IA de alto riesgo independientes

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contendrá la información prevista en el apartado 2 en relación con los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, registrados con arreglo al artículo 51.

2. Los proveedores introducirán en la base de datos de la UE los datos que se enumeran en el anexo VIII. La Comisión les prestará apoyo técnico y administrativo.

3. La información presente en la base de datos de la UE será accesible para el público.

4. La base de datos de la UE únicamente contendrá los datos personales que sean necesarios para la recogida y el tratamiento de información de conformidad con el presente Reglamento. Dicha información incluirá los nombres y datos de contacto de las personas físicas responsables del registro de sistema y que cuenten con autoridad legal para representar al proveedor.

5. La Comisión será la responsable del tratamiento de la base de datos de la UE. Velará por que los proveedores cuenten con un apoyo técnico y administrativo adecuado.

TÍTULO VIII

SEGUIMIENTO POSTERIOR A LA COMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN, VIGILANCIA DEL MERCADO

CAPÍTULO 1

SEGUIMIENTO POSTERIOR A LA COMERCIALIZACIÓN

Artículo 61

Seguimiento posterior a la comercialización por parte de los proveedores y plan de seguimiento posterior a la comercialización para sistemas de IA de alto riesgo

1. Los proveedores establecerán y documentarán un sistema de seguimiento posterior a la comercialización de forma proporcionada a la naturaleza de las tecnologías de inteligencia artificial y a los riesgos de los sistemas de IA de alto riesgo.

2. El sistema de seguimiento posterior a la comercialización recabará, documentará y analizará de manera activa y sistemática datos pertinentes proporcionados por usuarios o recopilados a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y permitirá al proveedor evaluar el cumplimiento de los requisitos establecidos en el título III, capítulo 2, por parte de los sistemas de IA.

3. El sistema de seguimiento posterior a la comercialización se basará en un plan de seguimiento posterior a la comercialización. El plan de seguimiento posterior a la comercialización formará parte de la documentación técnica a que se refiere el anexo IV. La Comisión adoptará un acto de ejecución en el que se establecerán disposiciones detalladas que constituyan un modelo para el plan de seguimiento posterior a la comercialización y la lista de elementos que deberán incluirse en él.

4. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos a que hace referencia el anexo II, cuando ya se hayan establecido un sistema y un plan de seguimiento posteriores a la comercialización con arreglo a dicha legislación, los elementos descritos en los apartados 1, 2 y 3 se integrarán en dicho sistema y plan, según proceda.

   El párrafo primero también se aplicará a los sistemas de IA de alto riesgo a que se refiere el punto 5, letra b), del anexo III introducidos en el mercado o puestos en servicio por entidades de crédito reguladas por la Directiva 2013/36/UE.

CAPÍTULO 2

INTERCAMBIO DE INFORMACIÓN SOBRE INCIDENTES Y FALLOS DE FUNCIONAMIENTO

Artículo 62

Notificación de incidentes graves y fallos de funcionamiento

1. Los proveedores de sistemas de IA de alto riesgo introducidos en el mercado de la Unión notificarán cualquier incidente grave o fallo de funcionamiento de dichos

sistemas que constituya un incumplimiento de las obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales a las autoridades de vigilancia del mercado de los Estados miembros donde se haya producido dicho incidente o incumplimiento.

Dicha notificación se efectuará inmediatamente después de que el proveedor haya establecido un vínculo causal entre el sistema de IA y el incidente o fallo de funcionamiento, o la posibilidad razonable de que exista dicho vínculo, y, en cualquier caso, a más tardar quince días después de que los proveedores tengan conocimiento de dicho incidente grave o fallo de funcionamiento.

2. Tras la recepción de la notificación relativa a un incumplimiento de las obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales, la autoridad de vigilancia del mercado informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 64, apartado 3. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1. Dichas orientaciones se publicarán en el plazo máximo de doce meses tras la entrada en vigor del presente Reglamento.

3. En el caso de los sistemas de IA de alto riesgo a que se refiere el punto 5, letra b), del anexo III introducidos en el mercado o puestos en servicio por proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE y en el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de dispositivos o que en sí mismos sean dispositivos, regulados por el Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746, la notificación de incidentes graves y fallos de funcionamiento se limitará a aquellos que constituyan un incumplimiento de las obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales.

CAPÍTULO 3

EJECUCIÓN

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 ejecución eficaz del presente Reglamento:

   a) se entenderá que toda referencia a un operador económico con arreglo al Reglamento (UE) 2019/1020 incluye a todos los operadores identificados en el título III, capítulo 3, del presente Reglamento;

   b) se entenderá que toda referencia a un producto con arreglo al Reglamento (UE) 2019/1020 incluye todos los sistemas de IA que estén comprendidos en el ámbito de aplicación del presente Reglamento.

2. La autoridad nacional de supervisión informará periódicamente a la Comisión sobre los resultados de las actividades pertinentes de vigilancia del mercado. La autoridad nacional de supervisión comunicará sin demora a la Comisión y a las autoridades nacionales de competencia pertinentes cualquier información recabada en el transcurso 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.

3. En el caso de los sistemas de IA de alto riesgo relacionados con productos a los que sean de aplicación los actos legislativos enumerados en el anexo II, sección A, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designadas en virtud de dichos actos legislativos.

4. En el caso de los sistemas de IA introducidos en el mercado, 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 pertinente responsable de la supervisión financiera de dichas entidades con arreglo a la mencionada legislación.

5. En el caso de los sistemas de IA enumerados en el punto 1, letra a), en la medida en que los sistemas se utilicen a los efectos de la aplicación de la ley, y en los puntos 6 y 7 del anexo III, los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control encargadas de la protección de datos con arreglo a la Directiva (UE) 2016/680 o el Reglamento 2016/679, o bien a las autoridades nacionales competentes responsables de supervisar las actividades de las autoridades encargadas de la aplicación de la ley o de las autoridades de inmigración o de asilo que pongan en servicio o utilicen dichos sistemas.

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.

7. Los Estados miembros facilitarán la coordinación entre las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento y otras autoridades u organismos nacionales pertinentes responsables de supervisar la aplicación de la legislación de armonización de la Unión citada en el anexo II u otra legislación de la Unión que pueda resultar pertinente para los sistemas de IA de alto riesgo a que se refiere el anexo III.

Artículo 64
Acceso a datos y documentación

1. Se concederá a las autoridades de vigilancia del mercado acceso a datos y documentación en el contexto de sus actividades, así como pleno acceso a los conjuntos de datos de entrenamiento, validación y prueba utilizados por el proveedor, incluso mediante interfaces de programación de aplicaciones («API», por sus siglas en inglés) u otros medios técnicos y herramientas adecuados que permitan el acceso a distancia.

2. En caso necesario y previa solicitud motivada, se concederá a las autoridades de vigilancia del mercado acceso al código fuente del sistema de IA para evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el título III, capítulo 2.

3. Las autoridades u organismos públicos nacionales encargados de supervisar o hacer respetar las obligaciones contempladas en el Derecho de la Unión en materia de protección de los derechos fundamentales con respecto al uso de sistemas de IA de alto riesgo mencionados en el anexo III tendrán la facultad de solicitar y acceder a

cualquier documentación creada o conservada con arreglo al presente Reglamento cuando el acceso a dicha documentación sea necesario para el ejercicio de las competencias derivadas de sus mandatos, dentro de los límites de su jurisdicción. La autoridad o el organismo público pertinente informará sobre dicha solicitud a la autoridad de vigilancia del mercado del Estado miembro que corresponda.

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 las enumerará en una lista pública disponible en el sitio web de la autoridad nacional de supervisión. Los Estados miembros notificarán dicha lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

5. Cuando la documentación mencionada en el apartado 3 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el 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 organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la estrecha colaboración de la autoridad u organismo público solicitante en un plazo razonable tras la presentación de la solicitud.

6. Cualquier información y documentación obtenidas por las autoridades u organismos públicos nacionales a que se refiere el apartado 3 con arreglo a las disposiciones recogidas en el presente artículo se tratarán de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 70.

Artículo 65

Procedimiento aplicable a los sistemas de IA que presenten un riesgo a nivel nacional

1. Los sistemas de IA que presenten un riesgo se entenderán como productos que presentan un riesgo según la definición del artículo 3, punto 19, del Reglamento (UE) 2019/1020 en lo que respecta a los riesgos para la salud, la seguridad o la protección de 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 según lo contemplado en el apartado 1, efectuará una evaluación del sistema de IA de que se trate para verificar su cumplimiento de todos los requisitos y obligaciones establecidos en el presente Reglamento. Cuando se presenten riesgos para la protección de 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. Los operadores pertinentes cooperarán en lo necesario con las autoridades 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 curso de tal evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá de inmediato al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos o bien retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo, que dicha autoridad prescriba.

La autoridad de vigilancia del mercado informará al organismo notificado correspondiente en consecuencia. El artículo 18 del Reglamento (UE) 2019/1020 será de aplicación a las medidas mencionadas 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 de los resultados de la evaluación y de las medidas que haya instado al operador a adoptar.

4. El operador se asegurará de que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en toda la Unión.

5. Si el operador de un sistema de IA no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema de IA en su mercado nacional, retirarlo de dicho mercado o recuperarlo. Dicha autoridad informará sin demora a la Comisión y a los demás Estados miembros de estas medidas.

6. La información mencionada en el apartado 5 incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación del sistema de IA no conforme, el origen del sistema de IA, la naturaleza de la presunta no conformidad y del riesgo planteado, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos formulados por el operador de que se trate. En particular, las autoridades de vigilancia del mercado indicarán si la no conformidad se debe a uno o varios de los motivos siguientes:

   a) el incumplimiento de los requisitos establecidos en el título III, capítulo 2, por parte del sistema de IA;

   b) deficiencias en las normas armonizadas o especificaciones comunes mencionadas en los artículos 40 y 41 que confieren la presunción de conformidad.

7. Las autoridades de vigilancia del mercado de los Estados miembros distintas de la autoridad de vigilancia del mercado del Estado miembro que inició el procedimiento comunicarán sin demora a la Comisión y a los demás Estados miembros toda medida que adopten y cualquier información adicional de que dispongan sobre la no conformidad del sistema de IA en cuestión y, en caso de desacuerdo con la medida nacional notificada, sus objeciones al respecto.

8. Si, en el plazo de tres meses desde la recepción de la información indicada en el apartado 5, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por un Estado miembro, la medida se considerará justificada. Esto se entiende sin perjuicio de los derechos procedimentales del operador correspondiente con arreglo al artículo 18 del Reglamento (UE) 2019/1020.

9. Las autoridades de vigilancia del mercado de todos los Estados miembros velarán por que se adopten sin demora las medidas restrictivas adecuadas respecto del producto de que se trate, tales como la retirada del producto del mercado.

Artículo 66
Procedimiento de salvaguardia de la Unión

1. Cuando, en el plazo de tres meses desde la recepción de la notificación indicada en el artículo 65, apartado 5, un Estado miembro formule objeciones sobre una medida adoptada por otro Estado miembro, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora con el Estado miembro y el operador u operadores pertinentes, y evaluará la medida nacional. Sobre la base de los resultados de la mencionada evaluación, la Comisión adoptará, en un plazo de nueve meses a partir de la notificación a que se refiere el artículo 65, apartado 5, una decisión en la que indicará si la medida nacional está justificada o no, y notificará dicha decisión al Estado miembro implicado.

2. Si la medida nacional se considera justificada, todos los Estados miembros adoptarán las medidas necesarias para garantizar la retirada de su mercado del sistema de IA no conforme e informarán a la Comisión en consecuencia. Si la medida nacional se considera injustificada, el Estado miembro implicado retirará la medida.

3. Cuando se considere que la medida nacional está justificada y la no conformidad del sistema de IA se atribuya a deficiencias de las normas armonizadas o especificaciones comunes a las que se refieren los artículos 40 y 41 del presente Reglamento, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) n.º 1025/2012.

Artículo 67
Sistemas de IA conformes que presenten un riesgo

1. Cuando, tras efectuar una evaluación con arreglo al artículo 65, la autoridad de vigilancia del mercado de un Estado miembro compruebe que un sistema de IA, aunque conforme con arreglo al presente Reglamento, presenta un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones en virtud del Derecho de la Unión o nacional destinadas a proteger los derechos fundamentales o para otros aspectos de protección del interés público, pedirá al operador correspondiente que adopte todas las medidas adecuadas para asegurarse de que el sistema de IA de que se trate ya no presente ese riesgo cuando se introduzca en el mercado o se ponga en servicio, o bien para retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo, que dicha autoridad determine.

2. El proveedor u otros operadores pertinentes se asegurarán de que se adoptan las medidas correctoras con respecto a todos los sistemas de IA afectados que hayan comercializado en toda la Unión en el plazo determinado por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. El Estado miembro informará inmediatamente a la Comisión y a los demás Estados miembros al respecto. La información facilitada incluirá todos los detalles disponibles, en particular los datos necesarios para identificar los sistemas de IA afectados y para determinar su origen, la cadena de suministro del sistema, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión consultará sin demora a los Estados miembros y al operador correspondiente y evaluará las medidas nacionales adoptadas. Sobre la base de los

resultados de la evaluación, la Comisión adoptará una decisión en la que indicará si la medida está justificada o no y, en su caso, propondrá medidas adecuadas.

5. La Comisión dirigirá su decisión a los Estados miembros.

Artículo 68
Incumplimiento formal

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro constate una de las situaciones indicadas a continuación, pedirá al proveedor correspondiente que subsane el incumplimiento de que se trate:

   a) la colocación del marcado de conformidad no es conforme con el artículo 49;

   b) no se ha colocado el marcado de conformidad;

   c) no se ha elaborado la declaración UE de conformidad;

   d) la declaración UE de conformidad no se ha elaborado correctamente;

   e) no se ha colocado, en su caso, el número de identificación del organismo notificado que interviene en el procedimiento de evaluación de la conformidad.

2. Si el incumplimiento indicado en el apartado 1 persiste, el Estado miembro correspondiente adoptará todas las medidas adecuadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o garantizar que se recupera o se retira del mercado.

TÍTULO IX

CÓDIGOS DE CONDUCTA

Artículo 69
Códigos de conducta

1. La Comisión y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta destinados a promover la aplicación voluntaria de los requisitos establecidos en el título III, capítulo 2, a sistemas de IA distintos de los de alto riesgo, sobre la base de especificaciones y soluciones técnicas que constituyan medios adecuados para garantizar el cumplimiento de dichos requisitos a la luz de la finalidad prevista de los sistemas.

2. La Comisión y el Comité fomentarán y facilitarán la elaboración de códigos de conducta destinados a promover la aplicación voluntaria a sistemas de IA de los requisitos relativos, por ejemplo, a la sostenibilidad ambiental, la accesibilidad para personas con discapacidad, la participación de partes interesadas en el diseño y desarrollo de los sistemas de IA y la diversidad de los equipos de desarrollo, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos.

3. Los códigos de conducta podrán ser elaborados por proveedores individuales de sistemas de IA, por organizaciones que los representen o por ambos, también con la participación de usuarios y de cualquier parte interesada y sus organizaciones representativas. Los códigos de conducta podrán abarcar uno o varios sistemas de IA, teniendo en cuenta la similitud de la finalidad prevista de los sistemas pertinentes.

4. La Comisión y el Comité tendrán en cuenta los intereses y necesidades específicos de los proveedores a pequeña escala y las empresas emergentes cuando fomenten y faciliten la elaboración de códigos de conducta.

TÍTULO X

CONFIDENCIALIDAD Y SANCIONES

Artículo 70
Confidencialidad

1. Las autoridades nacionales competentes y los organismos notificados involucrados en la aplicación del presente Reglamento respetarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades de modo que se protejan, en particular:

   a) los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos 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 eficaz del presente Reglamento, en particular a efectos de inspecciones, investigaciones o auditorías; c) los intereses públicos y de seguridad nacional;

   c) la integridad de las causas penales o los procedimientos administrativos.

2. Sin perjuicio de lo dispuesto en el apartado 1, la información intercambiada de forma confidencial entre las autoridades nacionales competentes y entre estas y la Comisión no se revelará sin consultar previamente a la autoridad nacional competente de origen y al usuario cuando las autoridades encargadas de la aplicación de la ley o las autoridades de inmigración o de asilo utilicen los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III y dicha divulgación pudiera comprometer los intereses públicos y de seguridad nacional.

   Cuando las autoridades encargadas de la aplicación de la ley o las autoridades de inmigración o de asilo sean proveedores de sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III, la documentación técnica mencionada en el anexo IV permanecerá dentro de las instalaciones 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 esta. Tan solo se permitirá acceder a dicha documentación o a cualquier copia de esta al personal de la autoridad de vigilancia del mercado que disponga de un nivel adecuado de habilitación de seguridad.

3. Los apartados 1 y 2 no afectarán a los derechos y obligaciones de la Comisión, los Estados miembros y los organismos notificados en lo que se refiere al intercambio de información y la difusión de advertencias, ni a las obligaciones de facilitar información que incumban a las partes interesadas en virtud del Derecho penal de los Estados miembros.

4. Cuando sea necesario, la Comisión y los Estados miembros podrán intercambiar información confidencial con autoridades reguladoras de terceros países con las que hayan celebrado acuerdos de confidencialidad bilaterales o multilaterales que garanticen un nivel de confidencialidad adecuado.

Artículo 71
Sanciones

1. De conformidad con los términos y condiciones establecidos en el presente Reglamento, los Estados miembros determinarán el régimen de sanciones, incluidas las multas administrativas, aplicable a las infracciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación adecuada y efectiva. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias. Tendrán particularmente en cuenta los intereses de los proveedores a pequeña escala y las empresas emergentes, así como su viabilidad económica.

2. Los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas y le notificarán, sin demora, cualquier modificación posterior de los mismos.

3. Las siguientes infracciones estarán sujetas a multas administrativas de hasta 30 000 000 EUR o, si el infractor es una empresa, de hasta el 6 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior:

   a) incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5;

   b) incumplimiento de los requisitos establecidos en el artículo 10 por parte del sistema de IA.

4. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento distintos de los dispuestos en los artículos 5 y 10 estará sujeto a multas administrativas de hasta 20 000 000 EUR o, si el infractor es una empresa, de hasta el 4 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior.

5. La presentación de información inexacta, incompleta o engañosa a organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 10 000 000 EUR o, si el infractor es una empresa, de hasta el 2 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior.

6. Al decidir la cuantía de la multa administrativa en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación correspondiente y se tendrá debidamente en cuenta lo siguiente:

   a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias;

   b) si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por la misma infracción;

   c) el tamaño y la cuota de mercado del operador que comete la infracción.

7. Cada Estado miembro establecerá normas que determinen si es posible, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. En función del ordenamiento jurídico de los Estados miembros, las normas relativas a las multas administrativas podrán aplicarse de tal modo que las multas las impongan órganos jurisdiccionales nacionales competentes u otros organismos, según proceda en dichos Estados miembros. La aplicación de dichas normas en estos Estados miembros tendrá un efecto equivalente.

Artículo 72

Multas administrativas a instituciones, agencias y organismos de la Unión

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, las agencias y los organismos de la Unión comprendidos en el ámbito de aplicación del presente Reglamento. Al decidir la imposición de una multa administrativa y su cuantía en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación de que se trate y se tendrá debidamente en cuenta lo siguiente:

   a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias;

   b) la cooperación con el Supervisor Europeo de Protección de Datos con el fin de poner remedio a la infracción y mitigar sus posibles efectos adversos, incluido el cumplimiento de cualquiera de las medidas que el propio Supervisor Europeo de Protección de Datos haya ordenado previamente contra la institución, agencia u organismo de la Unión de que se trate en relación con el mismo asunto;

   c) toda infracción anterior similar cometida por la institución, agencia u organismo de la Unión.

2. Las siguientes infracciones estarán sujetas a multas administrativas de hasta 500 000 EUR:

   a) incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5;

   b) incumplimiento de los requisitos establecidos en el artículo 10 por parte del sistema de IA.

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento distintos de los dispuestos en los artículos 5 y 10 será objeto de multas administrativas de hasta 250 000 EUR.

4. Antes de tomar ninguna decisión en virtud del presente artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución, agencia u organismo de la Unión sometida al procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de ser oída en lo que respecta a la posible infracción. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en los elementos y las circunstancias sobre las que las partes afectadas hayan podido manifestarse. Los denunciantes, si los hay, estarán estrechamente vinculadas al procedimiento.

5. Los derechos de defensa de las partes estarán garantizados plenamente en el curso del procedimiento. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas físicas y las empresas en la protección de sus datos personales o secretos comerciales.

6. La recaudación proveniente de la imposición de multas con arreglo al presente artículo pasará a engrosar los ingresos del presupuesto general de la Unión.

TÍTULO XI

DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

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. La delegación de poderes 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 otorgará a la Comisión por un periodo indefinido a partir de [*la fecha de entrada en vigor del Reglamento*].

3. La delegación de poderes 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, 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 especificada en dicha decisión. La decisión surtirá efecto al día siguiente 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. La Comisión, tan pronto como adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del 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, 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. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 74
Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado será de aplicación el artículo 5 del Reglamento (UE) n.º 182/2011.

TÍTULO XII

DISPOSICIONES FINALES

Artículo 75
Modificación del Reglamento (CE) n.º 300/2008

En el artículo 4, apartado 3, del Reglamento (CE) n.º 300/2008, se añade el párrafo siguiente:

«Al adoptar medidas detalladas relativas a las especificaciones técnicas y los procedimientos de aprobación y utilización del equipo de seguridad en relación con sistemas de inteligencia artificial en el sentido del Reglamento (UE) AAAA/XX [relativo a la 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) AAAA/XX [relativo a la inteligencia artificial] (DO ....).».

Artículo 76
Modificación del Reglamento (UE) n.º 167/2013

En el artículo 17, apartado 5, del Reglamento (UE) n.º 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) AAAA/XX [relativo a la 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) AAAA/XX [relativo a la inteligencia artificial] (DO ....).».

Artículo 77
Modificación del Reglamento (UE) n.º 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) AAAA/XX [relativo a la 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) AAAA/XX [relativo a la 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 apartado siguiente:

«4. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAA/XX [relativo a la inteligencia artificial] del Parlamento

Europeo y del Consejo*, la Comisión tendrá en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento al desempeñar sus actividades con arreglo al apartado 1 y al adoptar especificaciones técnicas y normas de ensayo de conformidad con los apartados 2 y 3.

_____

* Reglamento (UE) AAAA/XX [relativo a la 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 apartado siguiente:

«12. Al adoptar actos delegados en virtud del apartado 1 y actos de ejecución en virtud del apartado 11 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la 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) AAAA/XX [relativo a la inteligencia artificial] (DO ....).».

Artículo 80
Modificación del Reglamento (UE) 2018/858

En el artículo 5 del Reglamento (UE) 2018/858, se añade el apartado siguiente:

«4. 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) AAAA/XX [relativo a la 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) AAAA/XX [relativo a la inteligencia artificial] (DO ....).».

Artículo 81
Modificación del Reglamento (UE) 2018/1139

El Reglamento (UE) 2018/1139 se modifica como sigue:

1) En el artículo 17, se añade el apartado siguiente:

«3. Sin perjuicio de lo dispuesto en el apartado 2, al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [*relativo a la 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) AAAA/XX [relativo a la inteligencia artificial] (DO ....).».

2) En el artículo 19, se añade el apartado 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)

AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

3) En el artículo 43, se añade el apartado siguiente:

«4. Al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

4) 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) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

5) En el artículo 57, se añade el apartado siguiente:

«Al adoptar dichos actos de ejecución en relación con sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

6) En el artículo 58, se añade el apartado siguiente:

«3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la 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 apartado siguiente:

«3. Al adoptar los actos de ejecución en virtud del apartado 2 en relación con sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la 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) AAAA/XX [relativo a la inteligencia artificial] (DO ....).».

Artículo 83
Sistemas de IA ya introducidos en el mercado o puestos en servicio

1. El presente Reglamento no se aplicará a los sistemas de IA que sean componentes de sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo IX que hayan sido introducidos en el mercado o puestos en servicio antes de *[12 meses después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2]*, salvo que la sustitución o modificación de dichos actos legislativos redunde en un cambio significativo en el diseño o la finalidad prevista del sistema o sistemas de IA de que se trate.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta, en su caso, en la evaluación de cada sistema informático de gran magnitud establecido por los actos legislativos enumerados en el anexo IX que se efectúe de conformidad con dichos actos respectivos.

2. El presente Reglamento se aplicará a los sistemas de IA de alto riesgo distintos de los contemplados en el apartado 1 que hayan sido introducidos en el mercado o puestos en servicio antes de [*fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2*] únicamente si, a partir de dicha fecha, los sistemas mencionados se ven sometidos a cambios significativos en su diseño o su finalidad prevista.

Artículo 84
Evaluación y revisión

1. La Comisión evaluará la necesidad de modificar la lista que figura en el anexo III una vez al año a partir de la entrada en vigor del presente Reglamento.

2. A más tardar [*tres 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 presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

3. Los informes mencionados en el apartado 2 prestarán una atención especial a lo siguiente:

   a) el estado de los recursos financieros y humanos de las autoridades nacionales competentes para desempeñar de forma eficaz las funciones asignadas en virtud del presente Reglamento;

   b) el estado de las sanciones y, en particular, de las multas administrativas a que se refiere el artículo 71, apartado 1, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento.

4. En los [*tres años siguientes a la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2*] y posteriormente cada cuatro años, la Comisión evaluará el impacto y la eficacia de los códigos de conducta para promover la aplicación de los requisitos establecidos en el título III, capítulo 2, y en su caso otros requisitos adicionales, a los sistemas de IA distintos de los sistemas de IA de alto riesgo.

5. A efectos de lo dispuesto en los apartados 1 a 4, el Comité, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión a petición de esta.

6. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 a 4, la Comisión tendrá en cuenta las posiciones y conclusiones del Comité, el Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

7. La Comisión presentará, en caso necesario, las propuestas oportunas de modificación del presente Reglamento, en particular teniendo en cuenta la evolución de la tecnología y a la vista de los avances en la sociedad de la información.

Artículo 85
Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento se aplicará a partir de [veinticuatro meses tras la entrada en vigor del Reglamento].

3. No obstante lo dispuesto en el apartado 2:

   a) el título III, capítulo 4, y el título IV se aplicarán a partir de [*tres meses tras la entrada en vigor del presente Reglamento*];

   b) el artículo 71 se aplicará a partir de [doce meses tras la entrada en vigor del presente Reglamento].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente / La Presidenta*

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Ámbito(s) político(s) afectado(s)

1.3. La propuesta/iniciativa se refiere a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e incidencia esperados

1.4.4. Indicadores de resultados

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado del despliegue de la aplicación de la iniciativa

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

1.5.5 Evaluación de las diferentes opciones de financiación disponibles, en particular, posibilidades de reasignación

1.6. Duración e incidencia financiera de la propuesta/iniciativa

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema de gestión y de control

2.2.1. Justificación del modo o los modos de gestión, el mecanismo o los mecanismos de aplicación de la financiación, las modalidades de pago y la estrategia de control propuestos

2.2.2. Información relativa a los riesgos identificados y al sistema o los sistemas de control interno establecidos para mitigarlos

2.2.3. Estimación y justificación de la rentabilidad de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia financiera estimada de la propuesta sobre los créditos

3.2.1. Resumen de la incidencia estimada en los créditos de operaciones

3.2.2. Resultados estimados financiados con créditos de operaciones

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión

1.2. Ámbito(s) político(s) afectado(s)

Redes de comunicación, contenido y tecnologías;

Mercado interior, industria, emprendimiento y pymes;

La incidencia presupuestaria se refiere a las nuevas funciones encomendadas a la Comisión, incluido el respaldo al Comité Europeo de Inteligencia Artificial;

Actividad: configurar el futuro digital de Europa.

1.3. La propuesta/iniciativa se refiere a:

X **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto/una acción preparatoria**[64]

☐ **la prolongación de una acción existente**

☐ **una acción reorientada hacia una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

El objetivo general de la intervención es garantizar el adecuado funcionamiento del mercado interior mediante la creación de las condiciones necesarias para el desarrollo y uso de inteligencia artificial fiable en la Unión.

1.4.2. Objetivo(s) específico(s)

Objetivo específico n.º 1

Establecer requisitos específicos para los sistemas de IA y obligaciones a todos los participantes de la cadena de valor para garantizar que los sistemas de IA que se introducen en el mercado y se utilizan sean seguros y respeten la legislación vigente sobre los derechos fundamentales y los valores de la Unión.

Objetivo específico n.º 2

Garantizar la seguridad jurídica para facilitar la inversión e innovación en IA mediante la especificación de los requisitos y obligaciones esenciales y los procedimientos de conformidad y cumplimiento que deben seguirse para introducir o utilizar un sistema de IA en el mercado de la Unión.

Objetivo específico n.º 3

Mejorar la gobernanza y la aplicación efectiva de la legislación vigente sobre los derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA

[64] Tal como se contempla en el artículo 54, apartado 2, letras a) o b), del Reglamento Financiero

mediante la provisión de nuevas competencias, recursos y normas claras a las autoridades pertinentes en materia de procedimientos de evaluación de la conformidad y de control *a posteriori* y la división de las funciones de gobernanza y supervisión entre los niveles nacional y de la Unión.

Objetivo específico n.º 4

Facilitar el desarrollo de un mercado único de aplicaciones legales, seguras y fiables de la IA y evitar la fragmentación del mercado mediante la adopción de medidas a escala de la UE con el fin de fijar requisitos mínimos para que los sistemas de IA sean introducidos y utilizados en el mercado de la Unión de conformidad con la legislación vigente en materia de derechos fundamentales y seguridad.

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

Los proveedores de IA deberían beneficiarse de un conjunto de requisitos mínimos pero claros que generen seguridad jurídica y garanticen el acceso a todo el mercado único.

Los usuarios de la IA deberían beneficiarse de la seguridad jurídica que garantice que los sistemas de IA de alto riesgo que adquieran cumplen con el Derecho y los valores de la Unión.

Los consumidores deberían beneficiarse de una reducción del riesgo de vulneración de su seguridad o sus derechos fundamentales.

1.4.4. Indicadores de resultados

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

Indicador 1

Número de incidentes graves o resultados de la IA que constituyan un incidente grave o una violación de las obligaciones asociadas a los derechos fundamentales (semestral) por ámbito de aplicación y calculados a) en términos absolutos, b) como porcentaje de las aplicaciones utilizadas y c) como porcentaje de ciudadanos afectados.

Indicador 2

a) Inversión total en IA en la UE (anual)

b) Inversión total en IA por Estado miembro (anual)

c) Porcentaje de empresas que utilizan IA (anual)

d) Porcentaje de pymes que utilizan IA (anual)

Los puntos a) y b) se calcularán con base en fuentes oficiales y se compararán con estimaciones privadas.

Los puntos c) y d) se recabarán mediante encuestas periódicas a empresas.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado del despliegue de la aplicación de la iniciativa

El presente Reglamento debe ser plenamente aplicable un año y medio después de su fecha de adopción. No obstante, deben establecerse determinados elementos de la estructura de gobernanza con anterioridad. En particular, los Estados miembros deberán haber designado con anterioridad a autoridades existentes o establecido nuevas autoridades para desempeñar las funciones previstas en la legislación, y el Comité Europeo de Inteligencia Artificial deberá estar configurado y en funcionamiento. En el momento de la aplicabilidad, la base de datos europea sobre sistemas de IA debe estar plenamente operativa. Por lo tanto, es necesario desarrollar la base de datos de manera paralela al proceso de adopción, de modo que dicho desarrollo haya concluido en el momento de entrada en vigor del Reglamento.

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

El mosaico de normas nacionales con posibles divergencias que está surgiendo entorpecerá la provisión fluida de sistemas de IA en la UE y no garantizará la seguridad y la protección de los derechos fundamentales y los valores de la Unión en los distintos Estados miembros de manera efectiva. Una acción legislativa común de la UE en lo referente a la IA podría impulsar el mercado interior y tiene un gran potencial para proporcionar a la industria europea una ventaja competitiva en el panorama mundial y economías de escala que los Estados miembros no pueden lograr por sí solos.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La Directiva 2000/31/CE sobre comercio electrónico proporciona el marco principal para el funcionamiento del mercado interior y la supervisión de los servicios digitales y establece una estructura básica para un mecanismo general de cooperación entre los Estados miembros, que abarca en principio todos los requisitos aplicables a los servicios digitales. En la evaluación de la Directiva se señalaron deficiencias en varios aspectos de este mecanismo de cooperación, incluidos importantes aspectos relativos al procedimiento como la falta de plazos claros para la respuesta de los Estados miembros, junto con una falta general de respuesta a las solicitudes de sus homólogos. A lo largo de los años, esto ha generado desconfianza entre los Estados miembros para hacer frente a las inquietudes que suscitan los proveedores que ofrecen servicios digitales a través de las fronteras. La evaluación de la Directiva mostró la necesidad de definir un conjunto de reglas y requisitos diferenciados a nivel europeo. Por esta razón, la aplicación de las obligaciones específicas estipuladas en el presente Reglamento requeriría un mecanismo de cooperación específico a escala europea, con una estructura de gobernanza que garantice la coordinación de los órganos responsables específicos a escala europea.

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

El Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión define un nuevo marco común de requisitos aplicables a los sistemas de IA, que va más allá del marco establecido por la legislación vigente. Por este motivo, es necesario crear con esta propuesta una nueva función de regulación y coordinación nacional y europea.

En lo que respecta a sus posibles sinergias con otros instrumentos adecuados, la función de las autoridades notificantes a nivel nacional pueden desempeñarla autoridades nacionales que ejerzan funciones similares con arreglo a otros Reglamentos de la Unión.

Asimismo, al aumentar la confianza en la IA y, por tanto, fomentar la inversión en su desarrollo y adopción, se complementa el programa Europa Digital, que incluye entre sus cinco prioridades la promoción de la difusión de la IA.

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, en particular, posibilidades de reasignación

Se redistribuirá el personal. Los demás costes se sufragarán con cargo al presupuesto del programa Europa Digital, ya que el objetivo del presente Reglamento —garantizar una IA fiable— contribuye directamente a uno de los objetivos principales de dicho programa, a saber, acelerar el desarrollo y despliegue de la IA en Europa.

1.6. Duración e incidencia financiera de la propuesta/iniciativa

☐ **duración limitada**

– ☐ en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA

– ☐ incidencia financiera desde AAAA hasta AAAA para los créditos de compromiso y desde AAAA hasta AAAA para los créditos de pago.

X **duración ilimitada**

– ejecución con una fase de puesta en marcha de uno/dos (por confirmar) año(s),

– y pleno funcionamiento a partir de la última fecha.

1.7. Modo(s) de gestión previsto(s)[65]

X **Gestión directa** a cargo de la Comisión

– ☐ por sus departamentos, incluido su personal en las delegaciones de la Unión;

– ☐ por las agencias ejecutivas

☐ **Gestión compartida** con los Estados miembros

☐ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

– ☐ terceros países o los organismos que estos hayan designado;

– ☐ organizaciones internacionales y sus agencias (especifíquense);

– ☐ el BEI y el Fondo Europeo de Inversiones;

– ☐ los organismos a que se hace referencia en los artículos 70 y 71 del Reglamento Financiero;

– ☐ organismos de Derecho público;

– ☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;

– ☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la política exterior y de seguridad común (PESC), de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

– *Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.*

Observaciones

[65] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

El Reglamento se revisará y evaluará a los cinco años de su entrada en vigor. La Comisión informará sobre las conclusiones de la evaluación al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo.

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del modo o los modos de gestión, el mecanismo o los mecanismos de aplicación de la financiación, las modalidades de pago y la estrategia de control propuestos

El Reglamento establece una nueva política con respecto a normas armonizadas para la provisión de sistemas de inteligencia artificial en el mercado interior, al tiempo que garantiza el respeto de la seguridad y los derechos fundamentales. Estas nuevas normas requieren un mecanismo de coherencia para la aplicación transfronteriza de las obligaciones estipuladas en el presente Reglamento en forma de un nuevo grupo consultivo que coordine las actividades de las autoridades nacionales.

Para que puedan afrontar estas tareas, es necesario dotar de recursos apropiados a los servicios de la Comisión. Se calcula que la ejecución del nuevo Reglamento requerirá diez EJC en total (cinco EJC para el respaldo de las actividades del Comité y cinco EJC para el Supervisor Europeo de Protección de Datos, que actúa como organismo notificante para los sistemas de IA desplegados por parte de un organismo de la Unión Europea).

2.2.2. Información relativa a los riesgos identificados y al sistema o los sistemas de control interno establecidos para mitigarlos

A fin de asegurar que los miembros del Comité tengan la posibilidad de efectuar análisis con conocimiento de causa sobre la base de pruebas objetivas, se prevé que el Comité cuente con el apoyo de la estructura administrativa de la Comisión y que se cree un grupo de expertos para proporcionar conocimientos técnicos adicionales, si así se requiere.

2.2.3. Estimación y justificación de la rentabilidad de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

En lo relativo a los gastos de reuniones, debido al reducido valor por transacción (p. ej., el reembolso de los gastos de viaje de un delegado que participe en una reunión), los procedimientos de control normalizados parecen suficientes. En lo que respecta al desarrollo de la base de datos, la adjudicación de contratos cuenta con un sólido sistema de control interno en la DG CNECT mediante actividades de contratación centralizadas.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, en la estrategia de lucha contra el fraude.

Las medidas existentes de prevención del fraude aplicables a la Comisión cubrirán los créditos adicionales necesarios para el presente Reglamento.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

- Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[66]	de países de la AELC[67]	de países candidatos [68]	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
7	20 02 06 Gastos administrativos	CND	NO	NO	NO	NO
1	02 04 03 Programa Europa Digital relativo a la Inteligencia Artificial	CD	SÍ	NO	NO	NO
1	02 01 30 01 Gasto de apoyo para el programa Europa Digital	CND	SÍ	NO	NO	NO

3.2. Incidencia financiera estimada de la propuesta sobre los créditos

3.2.1. Resumen de la incidencia estimada sobre los gastos en los créditos de operaciones

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones

– X La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

En millones EUR (al tercer decimal)

[66] CD = créditos disociados / CND = créditos no disociados.

[67] AELC: Asociación Europea de Libre Comercio.

[68] Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

Rúbrica del marco financiero plurianual	1	

DG: CNECT				Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**[69]	**TOTAL**	
•Créditos de operaciones											
Línea presupuestaria[70] 02 04 03		Compromisos	(1a)		1,000						**1,000**
		Pagos	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Línea presupuestaria		Compromisos	(1b)								
		Pagos	(2b)								
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[71]											
Línea presupuestaria 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
TOTAL de los créditos para la DG CNECT		Compromisos	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Pagos	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 Indicativo y supeditado a las disponibilidades presupuestarias.

70 Según la nomenclatura presupuestaria oficial.

71 Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

• TOTAL de los créditos de operaciones	Compromisos	(4)		1,000						**1,000**
	Pagos	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
•TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
TOTAL de los créditos para la RÚBRICA 1 del marco financiero plurianual	Compromisos	=4+ 6		1,240	0,240	0,240	.0,240	0,240		**2,200**
	Pagos	=5+ 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Si la propuesta/iniciativa afecta a más de una rúbrica, repetir la sección anterior:

• TOTAL de los créditos de operaciones (todas las rúbricas operativas)	Compromisos	(4)								
	Pagos	(5)								
• TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos (todas las rúbricas operativas)		(6)								
TOTAL de los créditos para las RÚBRICAS 1 a 6 del marco financiero plurianual (Importe de referencia)	Compromisos	=4+ 6								
	Pagos	=5+ 6								

Rúbrica del marco financiero plurianual	**7**	«Gastos administrativos»

Esta sección debe rellenarse utilizando los «datos presupuestarios de carácter administrativo» que deben introducirse primero en el anexo de la ficha financiera legislativa (anexo V de las normas internas), que se carga en DECIDE a efectos de consulta entre servicios.

En millones EUR (al tercer decimal)

		Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**Después de 2027**[72]	**TOTAL**
DG: CNECT								
• Recursos humanos		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Otros gastos administrativos		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
TOTAL para la DG CNECT	**Créditos**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Supervisor Europeo de Protección de Datos								
• Recursos humanos		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Otros gastos administrativos								
TOTAL para el SEPD	**Créditos**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
TOTAL de los créditos para la RÚBRICA 7 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

En millones EUR (al tercer decimal)

	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**		**TOTAL**

[72] Todas las cifras de esta columna son indicativas y están sujetas a la continuidad de los programas y la disponibilidad de créditos.

TOTAL de los créditos para las RÚBRICAS 1 a 7 del marco financiero plurianual	Compromisos		2,770	1,770	1,770	1,770	1,770		**9,850**
	Pagos		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Resultados estimados financiados con créditos de operaciones

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados ⇩			Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		Después de **2027**[73]		**TOTAL**	
	RESULTADOS																	
	Tipo	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO N.º 1[74] …																		
Base de datos					1	1,000	1		1		1		1		1	0,100	1	1,000
Reuniones- Resultado					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Actividades de comunicación					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Subtotal del objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2 ...																		
- Resultado																		
Subtotal del objetivo específico n.º 2																		
TOTALES					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Todas las cifras de esta columna son indicativas y están sujetas a la continuidad de los programas y la disponibilidad de créditos.

[74] Tal como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…».

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

– ☐ La propuesta/iniciativa no exige la utilización de créditos de carácter administrativo.

– X La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**Anualmente a partir de 2027**[75]	**TOTAL**
HEADING 7 del marco financiero plurianual								
Recursos humanos		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Otros gastos administrativos		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Subtotal HEADING 7 del marco financiero plurianual		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Al margen de la RÚBRICA 7[76] **del marco financiero plurianual**								
Recursos humanos								
Otros gastos de carácter administrativo		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
TOTAL		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción y/o reasignados dentro de la DG, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

[75] Todas las cifras de esta columna son indicativas y están sujetas a la continuidad de los programas y la disponibilidad de créditos.

[76] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.3.1. Necesidades estimadas de recursos humanos

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

– X La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en unidades de equivalente a jornada completa

.		Año **2023**	Año **2024**	Año **2025**	**2026**	**2027**	**Después de 2027**[77]	
• Empleos de plantilla (funcionarios y personal temporal)								
20 01 02 01 (Sede y Oficinas de Representación de la Comisión)		10	10	10	10	10	10	
20 01 02 03 (Delegaciones)								
01 01 01 01 (Investigación indirecta)								
01 01 01 11 (Investigación directa)								
Otras líneas presupuestarias (especifíquense)								
• Personal externo (en unidades de equivalente a jornada completa: EJC)[78]								
20 02 01 (AC, ENCS, INT de la dotación global)								
20 02 03 (AC, AL, ENCS, INT y JED en las Delegaciones)								
XX 01 xx **yy zz**[79]	- en la sede							
	- en las delegaciones							
01 01 01 02 (AC, ENCS, INT; investigación indirecta)								
01 01 01 12 (AC, INT, ENCS; investigación directa)								
Otras líneas presupuestarias (especifíquense)								
TOTAL		**10**	**10**	**10**	**10**	**10**	**10**	

XX es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Se espera que el SEPD facilite la mitad de los recursos necesarios.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Para preparar un total de entre trece y dieciséis reuniones, proyectos de informes, continuar con el trabajo políticos, por ejemplo, relativo a futuras modificaciones de la lista de aplicaciones de IA de alto riesgo, y mantener relaciones con las autoridades de los Estados miembros, se necesitarán cuatro AD EJC y un AST EJC. El Supervisor Europeo de Protección de Datos es responsable de los sistemas de IA desarrollados por las instituciones de la UE. A partir de la experiencia acumulada, puede estimarse que se requerirán cinco AD EJC para desempeñar las

[77] Todas las cifras de esta columna son indicativas y están sujetas a la continuidad de los programas y la disponibilidad de créditos.

[78] AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JPD = joven profesional en delegación.

[79] Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

	responsabilidades del SEPD con arreglo al proyecto de legislación.
Personal externo	

3.2.4. Compatibilidad con el marco financiero plurianual vigente

La propuesta/iniciativa:

– X puede ser financiada en su totalidad mediante una redistribución dentro de la rúbrica correspondiente del marco financiero plurianual (MFP).

No se requiere reprogramación.

– ☐ requiere el uso del margen no asignado con cargo a la rúbrica pertinente del MFP y/o el uso de los instrumentos especiales tal como se define en el Reglamento del MFP.

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas, los importes correspondientes y los instrumentos cuya utilización se propone.

– ☐ requiere una revisión del MFP.

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas y los importes correspondientes.

3.2.5. Contribución de terceros

La propuesta/iniciativa:

– X no prevé la cofinanciación por parte de terceros

– ☐ prevé la cofinanciación por parte de terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**[80]	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

[80] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de aplicación previsto (por ejemplo: 2021). Hágase lo mismo con los años siguientes.

3.3. Incidencia estimada en los ingresos

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

– ☐ en otros ingresos

– ☐ en otros ingresos

– Indíquese si los ingresos se asignan a las líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[81]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo ….								

En el caso de los ingresos asignados, especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

Otras observaciones (por ejemplo, método/fórmula que se utiliza para calcular la incidencia sobre los ingresos o cualquier otra información).

[81] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos una vez deducido el 20 % de los gastos de recaudación.