2024/1689

12.7.2024

REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 13 de junio de 2024

por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

(Texto pertinente a efectos del EEE)

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 ([1]),

Visto el dictamen del Banco Central Europeo ([2]),

Visto el dictamen del Comité de las Regiones ([3]),

De conformidad con el procedimiento legislativo ordinario ([4]),

Considerando lo siguiente:

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial (en lo sucesivo, «sistemas de IA») en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación. El presente Reglamento garantiza la libre circulación transfronteriza de mercancías 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) El presente Reglamento debe aplicarse de conformidad con los valores de la Unión consagrados en la Carta, lo que facilitará la protección de las personas físicas, las empresas, la democracia, el Estado de Derecho y la protección del medio ambiente y, al mismo tiempo, impulsará la innovación y el empleo y convertirá a la Unión en líder en la adopción de una IA fiable.

(3) Los sistemas de IA pueden desplegarse con facilidad en sectores muy diversos de la economía y en muchas partes de la sociedad, también a escala transfronteriza, y circular fácilmente por toda la Unión. Algunos Estados miembros ya han estudiado adopción de normas nacionales destinadas a garantizar que la IA sea fiable y segura y se desarrolle y utilice de conformidad con las obligaciones relativas a los derechos fundamentales. La existencia de normas nacionales divergentes puede dar lugar a la fragmentación del mercado interior y reducir la seguridad jurídica de los operadores que desarrollan, importan o utilizan sistemas de IA. Por lo tanto, es preciso garantizar un nivel elevado y coherente de protección en toda la Unión para lograr una IA fiable, así como evitar las divergencias que obstaculizan la libre circulación, la innovación, el despliegue y la adopción en el mercado interior de los sistemas de IA y los

([1]) DO C 517 de 22.12.2021, p. 56.
([2]) DO C 115 de 11.3.2022, p. 5.
([3]) DO C 97 de 28.2.2022, p. 60.
([4]) Posición del Parlamento Europeo de 13 de marzo de 2024 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 21 de mayo de 2024.

productos y servicios conexos mediante el establecimiento de obligaciones uniformes para los operadores y la garantía de 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 con fines de garantía del cumplimiento del Derecho, el uso de sistemas de IA para la realización de evaluaciones de riesgos de personas físicas con fines de garantía del cumplimiento del Derecho y el uso de sistemas de IA de categorización biométrica con fines de garantía del cumplimiento del Derecho, 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 del recurso al artículo 16 del TFUE, conviene consultar al Comité Europeo de Protección de Datos.

(4) La IA es un conjunto de tecnologías en rápida evolución que contribuye a generar beneficios económicos, medioambientales y sociales muy diversos en todos los sectores económicos y las actividades sociales. El uso de la IA 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 seguridad alimentaria, la educación y la formación, los medios de comunicación, el deporte, la cultura, la gestión de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, el seguimiento ambiental, la conservación y restauración de la biodiversidad y los ecosistemas, 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.

(5) Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos, la IA puede generar riesgos y menoscabar los intereses públicos y los derechos fundamentales que protege el Derecho de la Unión. Dicho menoscabo puede ser tangible o intangible e incluye los perjuicios físicos, psíquicos, sociales o económicos.

(6) Dadas las importantes repercusiones que la IA puede tener en la sociedad y la necesidad de generar confianza, es fundamental que la IA y su marco reglamentario se desarrollen de conformidad con los valores de la Unión consagrados en el artículo 2 del Tratado de la Unión Europea (TUE), los derechos y libertades fundamentales consagrados en los Tratados y, de conformidad con el artículo 6 del TUE, la Carta. Como requisito previo, la IA debe ser una tecnología centrada en el ser humano. Además, debe ser una herramienta para las personas y tener por objetivo último aumentar el bienestar humano.

(7) Conviene establecer normas comunes para 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. Estas normas deben ser coherentes con la Carta, no deben ser discriminatorias y deben estar en consonancia con los compromisos de la Unión en materia de comercio internacional. También deben tener en cuenta la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital y las Directrices éticas para una IA fiable del Grupo independiente de expertos de alto nivel sobre inteligencia artificial.

(8) En consecuencia, se necesita un marco jurídico de la Unión que establezca unas normas armonizadas en materia de IA para impulsar el desarrollo, la utilización y la adopción en el mercado interior de la IA y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado, la puesta en servicio y la utilización de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de libre circulación de mercancías y servicios. Esas normas deben ser claras y firmes por lo que respecta a proteger los derechos fundamentales, apoyar nuevas soluciones innovadoras, posibilitar un ecosistema europeo de agentes públicos y privados que creen sistemas de IA en consonancia con los valores de la Unión y liberar el potencial de la transformación digital en todas las regiones de la Unión. Al establecer tales normas, así como medidas en apoyo de la innovación que prestan especial atención a las pequeñas y medianas empresas (pymes), incluidas las empresas emergentes, el presente Reglamento respalda el objetivo de promover el enfoque europeo de la IA centrado en el ser humano y de ser un líder mundial en el desarrollo de IA segura, digna de confianza y ética, como indicó el Consejo Europeo ([5]), y garantiza la protección de los principios éticos, como solicitó específicamente el Parlamento Europeo ([6]).

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

(9) Deben establecerse normas armonizadas aplicables a la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA de alto riesgo en consonancia con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([7]), la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo ([8]) y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo ([9]) (en lo sucesivo, «nuevo marco legislativo»). Las normas armonizadas que se establecen en el presente Reglamento deben aplicarse en todos los sectores y, en consonancia con el nuevo marco legislativo, deben entenderse sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo, protección de los trabajadores y seguridad de los productos, al que complementa el presente Reglamento. En consecuencia, permanecen inalterados y siguen siendo plenamente aplicables todos los derechos y vías de recurso que el citado Derecho de la Unión otorga a los consumidores y demás personas que puedan verse afectados negativamente por los sistemas de IA, también en lo que respecta a la reparación de los posibles daños de conformidad con la Directiva 85/374/CEE del Consejo ([10]). Además, en el contexto del empleo y la protección de los trabajadores, el presente Reglamento no debe afectar, por tanto, al Derecho de la Unión en materia de política social ni al Derecho laboral nacional —de conformidad con el Derecho de la Unión— relativa a las condiciones de empleo y de trabajo, incluidas la salud y seguridad en el trabajo y la relación entre empleadores y trabajadores. El presente Reglamento tampoco debe afectar en modo alguno al ejercicio de los derechos fundamentales reconocidos en los Estados miembros y a escala de la Unión, incluidos el derecho o la libertad de huelga o de emprender otras acciones contempladas en los sistemas de relaciones laborales específicos de los Estados miembros y el derecho a negociar, concluir y hacer cumplir convenios colectivos o a llevar a cabo acciones colectivas conforme al Derecho nacional. El presente Reglamento no debe afectar a las disposiciones destinadas a mejorar las condiciones laborales en el trabajo en plataformas digitales establecidas en una Directiva del Parlamento Europeo y del Consejo relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales. Además, el presente Reglamento tiene por objeto reforzar la eficacia de tales derechos y vías de recurso vigentes mediante el establecimiento de requisitos y obligaciones específicos, también en lo que respecta a la transparencia, la documentación técnica y la conservación de registros de los sistemas de IA. Asimismo, las obligaciones impuestas a los distintos operadores que participan en la cadena de valor de la IA en virtud del presente Reglamento deben aplicarse sin perjuicio del Derecho nacional que, de conformidad con el Derecho de la Unión, tenga por efecto limitar el uso de determinados sistemas de IA cuando dicho Derecho quede fuera del ámbito de aplicación del presente Reglamento o persiga objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Así, por ejemplo, el presente Reglamento no debe afectar al Derecho laboral nacional ni al Derecho en materia de protección de menores, a saber, de personas de menos de dieciocho años, que tienen en cuenta la Observación general n.º 25 (2021) de la Convención sobre los Derechos del Niño de las Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital, en la medida en que no son específicas a los sistemas de IA y persiguen otros objetivos legítimos de interés público.

(10) El derecho fundamental a la protección de los datos personales está garantizado, en particular, por los Reglamentos (UE) 2016/679 ([11]) y (UE) 2018/1725 ([12]) del Parlamento Europeo y del Consejo y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([13]). Además, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([14]) protege la vida privada y la confidencialidad de las comunicaciones, también estableciendo condiciones para cualquier almacenamiento de datos personales y no personales en los equipos terminales, y el acceso desde estos. Dichos actos legislativos de la Unión constituyen la base para un tratamiento de datos sostenible y responsable, también cuando los conjuntos de datos contengan una combinación de datos personales y no personales. El presente Reglamento no pretende afectar a la aplicación del Derecho de la Unión vigente que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de supervisión independientes competentes para vigilar el cumplimiento de dichos instrumentos. Tampoco afecta a las obligaciones de los proveedores y los responsables del despliegue de sistemas de IA en su papel de responsables o encargados del tratamiento de datos

([7]) 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 por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

([8]) 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).

([9]) 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 (DO L 169 de 25.6.2019, p. 1).

([10]) Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (DO L 210 de 7.8.1985, p. 29).

([11]) 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).

([12]) 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).

([13]) 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 (DO L 119 de 4.5.2016, p. 89).

([14]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

derivadas del Derecho de la Unión o nacional en materia de protección de datos personales en la medida en que el diseño, el desarrollo o el uso de sistemas de IA impliquen el tratamiento de datos personales. También conviene aclarar que los interesados siguen disfrutando de todos los derechos y garantías que les confiere dicho Derecho de la Unión, incluidos los derechos relacionados con las decisiones individuales totalmente automatizadas, como la elaboración de perfiles. Unas normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA establecidas en virtud del presente Reglamento deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por el Derecho de la Unión en materia de protección de datos personales, así como de otros derechos fundamentales.

(11) El presente Reglamento debe interpretarse sin perjuicio de las disposiciones del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo ([15]) relativas a la responsabilidad de los prestadores de servicios intermediarios.

(12) Debe definirse con claridad el concepto de «sistema de IA» en el presente Reglamento y armonizarlo estrechamente con los trabajos de las organizaciones internacionales que se ocupan de la IA, a fin de garantizar la seguridad jurídica y facilitar la convergencia a escala internacional y una amplia aceptación, al mismo tiempo que se prevé la flexibilidad necesaria para dar cabida a los rápidos avances tecnológicos en este ámbito. Además, la definición debe basarse en las principales características de los sistemas de IA que los distinguen de los sistemas de *software* o los planteamientos de programación tradicionales y más sencillos, y no debe incluir los sistemas basados en las normas definidas únicamente por personas físicas para ejecutar automáticamente operaciones. Una característica principal de los sistemas de IA es su capacidad de inferencia. Esta capacidad de inferencia se refiere al proceso de obtención de resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos y virtuales, y a la capacidad de los sistemas de IA para deducir modelos o algoritmos, o ambos, a partir de información de entrada o datos. Las técnicas que permiten la inferencia al construir un sistema de IA incluyen estrategias de aprendizaje automático que aprenden de los datos cómo alcanzar determinados objetivos y estrategias basadas en la lógica y el conocimiento que infieren a partir de conocimientos codificados o de una representación simbólica de la tarea que debe resolverse. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización. El término «basado en una máquina» se refiere al hecho de que los sistemas de IA se ejecutan en máquinas.La referencia a objetivos explícitos o implícitos subraya que los sistemas de IA pueden funcionar con arreglo a objetivos definidos explícitos o a objetivos implícitos. Los objetivos del sistema de IA pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico. A los efectos del presente Reglamento, debe entenderse por entornos los contextos en los que funcionan los sistemas de IA, mientras que los resultados de salida generados por el sistema de IA reflejan las distintas funciones desempeñadas por los sistemas de IA e incluyen predicciones, contenidos, recomendaciones o decisiones. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso. Los sistemas de IA pueden utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente del producto (integrado) o contribuye a la funcionalidad del producto sin formar parte de él (no integrado).

(13) El concepto de «responsable del despliegue» a que hace referencia el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida cualquier autoridad pública, órgano u organismo, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del responsable del despliegue.

(14) El concepto de «datos biométricos» empleado en el presente Reglamento debe interpretarse a la luz del concepto de «datos biométricos» tal como se define en el artículo 4, punto 14, del Reglamento (UE) 2016/679, en el artículo 3, punto 18, del Reglamento (UE) 2018/1725, y en el artículo 3, punto 13, de la Directiva (UE) 2016/680. Los datos biométricos pueden permitir la autenticación, la identificación o la categorización de las personas físicas y el reconocimiento de las emociones de las personas físicas.

(15) El concepto de «identificación biométrica» a que hace referencia el presente Reglamento debe definirse como el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento. Quedan excluidos los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local.

([15]) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO L 277 de 27.10.2022, p. 1).

(16) El concepto de «categorización biométrica» a que hace referencia el presente Reglamento debe definirse como la inclusión de personas físicas en categorías específicas en función de sus datos biométricos. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos conductuales o de la personalidad, la lengua, la religión, la pertenencia a una minoría nacional o la orientación sexual o política. No se incluyen los sistemas de categorización biométrica que sean una característica meramente accesoria intrínsecamente vinculada a otro servicio comercial, lo que significa que la característica no puede utilizarse, por razones técnicas objetivas, sin el servicio principal y que la integración de dicha característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas del presente Reglamento. Por ejemplo, los filtros que clasifican las características faciales o corporales utilizados en los mercados en línea podrían constituir una característica accesoria de este tipo, ya que solo pueden utilizarse en relación con el servicio principal, que consiste en vender un producto permitiendo al consumidor previsualizar cómo le quedaría y ayudarlo a tomar una decisión de compra. Los filtros utilizados en los servicios de redes sociales que clasifican las características faciales o corporales a fin de que los usuarios puedan añadir o modificar imágenes o vídeos también podrían considerarse una característica accesoria, ya que dichos filtros no pueden utilizarse sin el servicio principal de las redes sociales, que consiste en compartir contenidos en línea.

(17) El concepto de «sistema de identificación biométrica remota» a que hace referencia el presente Reglamento debe definirse de manera funcional como un sistema de IA destinado a identificar a personas físicas sin su participación activa, generalmente a distancia, comparando sus datos biométricos con los que figuren en una base de datos de referencia, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen. Estos sistemas de identificación biométrica remota suelen utilizarse para detectar a varias personas o su comportamiento de forma simultánea, a fin de simplificar considerablemente la identificación de personas sin su participación activa. Quedan excluidos los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local. Esa exclusión se justifica por el hecho de que tales sistemas probablemente tengan una repercusión menor en los derechos fundamentales de las personas físicas que los sistemas de identificación biométrica remota que puedan utilizarse para el tratamiento de los datos biométricos de un gran número de personas sin su participación activa. En el caso de los sistemas «en tiempo real», la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, casi instantánea o, en cualquier caso, sin una importante demora. 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 de que se trate generando demoras mínimas. Los sistemas «en tiempo real» implican el uso de materiales «en directo» o «casi en directo», como grabaciones de vídeo, generados por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas «en diferido» ya se han recabado los datos biométricos y la comparación e identificación se producen con una importante demora. A tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, generados con anterioridad a la utilización del sistema en relación con las personas físicas afectadas.

(18) El concepto de «sistema de reconocimiento de emociones» a que hace referencia el presente Reglamento debe definirse como un sistema de IA destinado a distinguir o deducir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos. El concepto se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión. No incluye los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se utilicen para distinguir o deducir emociones. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro.

(19) A los efectos del presente Reglamento, debe entenderse que el concepto de «espacio de acceso público» se refiere a cualquier espacio físico al que pueda acceder un número indeterminado de personas físicas y con independencia de si es de propiedad privada o pública y de la actividad para la que pueda utilizarse el espacio, ya sean actividades comerciales, por ejemplo, tiendas, restaurantes, cafeterías; de prestación de servicios, por ejemplo, bancos, actividades profesionales, hostelería; deportivas, por ejemplo, piscinas, gimnasios, estadios; de transporte, por ejemplo, estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte; de entretenimiento, por ejemplo, cines, teatros, museos, salas de conciertos, salas de conferencias; de ocio o de otro tipo, por ejemplo, vías y plazas públicas, parques, bosques, parques infantiles. Asimismo, debe considerarse que un espacio es de acceso público si, con independencia de posibles restricciones de capacidad o de seguridad, el acceso está sujeto a determinadas condiciones previamente definidas que puede satisfacer un número indeterminado de personas, como la adquisición de una entrada o un título de transporte, el registro previo o tener una determinada edad. Por el contrario, un espacio no debe considerarse de acceso público si únicamente pueden acceder a él determinadas personas físicas definidas, ya sea en virtud del Derecho de la Unión o del Derecho nacional directamente relacionado con la seguridad pública o en virtud de una clara manifestación de voluntad de la persona que ejerza la autoridad

pertinente sobre dicho espacio. La posibilidad real de acceso, como una puerta no cerrada con llave o una verja abierta, no implica por sí sola que el espacio sea de acceso público si hay indicios o circunstancias que sugieran lo contrario, como señales que prohíban o restrinjan el acceso. Los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que solo se pretende que accedan los empleados y proveedores de servicios pertinentes, no son espacios de acceso público. No deben incluirse en los espacios de acceso público las prisiones ni las zonas en que se realizan inspecciones fronterizas. Algunos espacios pueden incluir tanto zonas de acceso público como zonas que no son de acceso público, como los aeropuertos o el vestíbulo de un edificio residencial privado por el que se accede a una consulta médica. Los espacios en línea no son lugares de acceso público, ya que no son espacios físicos. 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.

(20) Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y de posibilitar el control democrático, la alfabetización en materia de IA debe dotar a los proveedores, responsables del despliegue y personas afectadas de los conceptos necesarios para tomar decisiones con conocimiento de causa en relación con los sistemas de IA. Esos conceptos pueden variar en función del contexto pertinente e incluir el entendimiento de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar los resultados de salida del sistema de IA y, en el caso de las personas afectadas, los conocimientos necesarios para comprender el modo en que las decisiones adoptadas con la ayuda de la IA tendrán repercusiones para ellas. En el contexto de la aplicación del presente Reglamento, la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución. Además, la puesta en práctica general de medidas de alfabetización en materia de IA y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo y, en última instancia, sostener la consolidación y la senda de innovación de una IA fiable en la Unión. El Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA») debe apoyar a la Comisión para promover las herramientas de alfabetización en materia de IA, la sensibilización pública y la comprensión de los beneficios, los riesgos, las salvaguardias, los derechos y las obligaciones en relación con el uso de sistemas de IA. En cooperación con las partes interesadas pertinentes, la Comisión y los Estados miembros deben facilitar la elaboración de códigos de conducta voluntarios para promover la alfabetización en materia de IA entre las personas que se ocupan del desarrollo, el manejo y el uso de la IA.

(21) 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 responsables del despliegue de sistemas de IA establecidos en la Unión.

(22) 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. Esto sucede, por ejemplo, cuando un operador establecido en la Unión firma con un operador establecido en un tercer país un contrato para la prestación de determinados servicios en relación con una actividad que llevará a cabo un sistema de IA que se consideraría de alto riesgo. En dichas circunstancias, el sistema de IA usado en un tercer país por el operador podría tratar datos recabados lícitamente en la Unión y transferidos desde su territorio, y proporcionar al operador contratante ubicado en la Unión los resultados de salida generados por dicho sistema de IA a raíz de este tratamiento sin que el sistema de IA de que se trate se introduzca en el mercado, se ponga en servicio o se utilice en la Unión. Para evitar la elusión de este Reglamento y garantizar la protección efectiva de las personas físicas ubicadas en la Unión, el presente Reglamento también debe aplicarse a los proveedores y responsables del despliegue de sistemas de IA establecidos en un tercer país, en la medida en que los resultados de salida generados por dichos sistemas estén destinados a utilizarse en la Unión. No obstante, con el objetivo de tener en cuenta los acuerdos existentes y las necesidades especiales de cooperación futura 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 organizaciones internacionales cuando actúen en el marco de acuerdos internacionales o de cooperación celebrados a escala nacional o de la Unión con fines de cooperación policial y judicial con la Unión o sus Estados miembros si el tercer país o la organización internacional correspondiente ofrece garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas. Cuando proceda, ello podrá incluir las actividades de entidades a las que los terceros países hayan encomendado tareas específicas en apoyo de dicha cooperación policial y judicial. Dichos marcos de cooperación o acuerdos se han establecido bilateralmente entre los Estados miembros y terceros países o entre la Unión Europea, Europol y otros órganos de la Unión y terceros países y organizaciones internacionales. Las autoridades competentes para la supervisión de las autoridades policiales y judiciales en virtud del presente Reglamento deben evaluar si dichos marcos de cooperación o acuerdos internacionales incluyen garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas. Las autoridades nacionales y las instituciones, órganos y organismos de la Unión que sean destinatarios de dichos resultados de salida y que la utilicen en la Unión siguen siendo responsables de garantizar que su utilización de la

información está en consonancia con el Derecho de la Unión. Cuando, en el futuro, dichos acuerdos internacionales se revisen o se celebren otros nuevos, las partes contratantes deben hacer todo lo posible por que dichos acuerdos se ajusten a los requisitos del presente Reglamento.

(23) El presente Reglamento también debe aplicarse a las instituciones, órganos y organismos de la Unión cuando actúen como proveedores o responsables del despliegue de un sistema de IA.

(24) En caso de que, y en la medida en que, los sistemas de IA se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificación, con fines militares, de defensa o de seguridad nacional, deben excluirse del ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades, por ejemplo, con independencia de que se trate de una entidad pública o de una entidad privada. Por lo que respecta a los fines militares y de defensa, dicha exclusión está justificada tanto por el artículo 4, apartado 2, del TUE como por las especificidades de la política de defensa de los Estados miembros y de la política común de defensa de la Unión a que se refiere el título V, capítulo 2, del TUE, que están sujetas al Derecho internacional público que, por lo tanto, es el marco jurídico más adecuado para la regulación de los sistemas de IA en el contexto del uso de la fuerza letal y de otros sistemas de IA en el contexto de las actividades militares y de defensa. Por lo que respecta a los fines de seguridad nacional, la exclusión está justificada tanto por el hecho de que la seguridad nacional sigue siendo responsabilidad exclusiva de los Estados miembros de conformidad con el artículo 4, apartado 2, del TUE, como por la naturaleza específica y las necesidades operativas de las actividades de seguridad nacional y por las normas nacionales específicas aplicables a dichas actividades. No obstante, si un sistema de IA desarrollado, introducido en el mercado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional se utilizara temporal o permanentemente fuera de estos ámbitos con otros fines (por ejemplo, con fines civiles o humanitarios, de garantía del cumplimiento del Derecho o de seguridad pública), dicho sistema entraría en el ámbito de aplicación del presente Reglamento. En tal caso, la entidad que utilice el sistema de IA con fines que no sean militares, de defensa o de seguridad nacional debe garantizar que el sistema de IA cumple lo dispuesto en el presente Reglamento, a menos que el sistema ya lo haga. Los sistemas de IA introducidos en el mercado o puestos en servicio para un fin excluido, a saber, militar, de defensa o de seguridad nacional, y uno o varios fines no excluidos, como fines civiles o de garantía del cumplimiento del Derecho, entran en el ámbito de aplicación del presente Reglamento y los proveedores de dichos sistemas deben garantizar el cumplimiento del presente Reglamento. En esos casos, el hecho de que un sistema de IA pueda entrar en el ámbito de aplicación del presente Reglamento no debe afectar a la posibilidad de que las entidades que llevan a cabo actividades militares, de defensa y de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades, utilicen sistemas de IA con fines de seguridad nacional, militares y de defensa, cuyo uso está excluido del ámbito de aplicación del presente Reglamento. Un sistema de IA introducido en el mercado con fines civiles o de garantía del cumplimiento del Derecho que se utilice, con o sin modificaciones, con fines militares, de defensa o de seguridad nacional no debe entrar en el ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades.

(25) El presente Reglamento debe apoyar la innovación, respetar la libertad de ciencia y no socavar la actividad de investigación y desarrollo. Por consiguiente, es necesario excluir de su ámbito de aplicación los sistemas y modelos de IA desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos. Además, es necesario garantizar que el presente Reglamento no afecte de otro modo a la actividad de investigación y desarrollo científicos sobre sistemas o modelos de IA antes de su introducción en el mercado o su puesta en servicio. Por lo que se refiere a la actividad de investigación, prueba y desarrollo orientada a productos en relación con sistemas o modelos de IA, las disposiciones del presente Reglamento tampoco deben aplicarse antes de que dichos sistemas y modelos se pongan en servicio o se introduzcan en el mercado. Esa exclusión se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando se introduzca en el mercado o se ponga en servicio como resultado de dicha actividad de investigación y desarrollo un sistema de IA que entre en el ámbito de aplicación del presente Reglamento, así como de la aplicación de disposiciones sobre espacios controlados de pruebas para la IA y pruebas en condiciones reales. Además, sin perjuicio de la exclusión de los sistemas de IA desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos, cualquier otro sistema de IA que pueda utilizarse para llevar a cabo cualquier actividad de investigación y desarrollo debe seguir estando sujeto a las disposiciones del presente Reglamento. En cualquier caso, toda actividad de investigación y desarrollo debe llevarse a cabo de conformidad con normas éticas y profesionales reconocidas para la investigación científica y con el Derecho aplicable de la Unión.

(26) Con el fin de establecer un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, es preciso aplicar un enfoque basado en los riesgos claramente definido, que adapte el tipo y contenido de las normas a la intensidad y el alcance de los riesgos que puedan generar los sistemas de IA de que se trate. Por consiguiente, es necesario prohibir determinadas prácticas de IA que no son aceptables, definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, así como imponer obligaciones de transparencia a determinados sistemas de IA.

(27) Si bien el enfoque basado en el riesgo es la base de un conjunto proporcionado y eficaz de normas vinculantes, es importante recordar las Directrices éticas para una IA fiable, de 2019, elaboradas por el Grupo independiente de expertos de alto nivel sobre IA creado por la Comisión. En dichas directrices, el Grupo independiente de expertos de alto nivel sobre IA desarrolló siete principios éticos no vinculantes para la IA que tienen por objeto contribuir a garantizar la fiabilidad y el fundamento ético de la IA. Los siete principios son: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas. Sin perjuicio de los requisitos jurídicamente vinculantes del presente Reglamento y de cualquier otro acto aplicable del Derecho de la Unión, esas directrices contribuyen al diseño de una IA coherente, fiable y centrada en el ser humano, en consonancia con la Carta y con los valores en los que se fundamenta la Unión. De acuerdo con las directrices del Grupo independiente de expertos de alto nivel sobre IA, por «acción y supervisión humanas» se entiende que los sistemas de IA se desarrollan y utilizan como herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que pueda ser controlada y vigilada adecuadamente por seres humanos. Por «solidez técnica y seguridad» se entiende que los sistemas de IA se desarrollan y utilizan de manera que sean sólidos en caso de problemas y resilientes frente a los intentos de alterar el uso o el funcionamiento del sistema de IA para permitir su uso ilícito por terceros y reducir al mínimo los daños no deseados. Por «gestión de la privacidad y de los datos» se entiende que los sistemas de IA se desarrollan y utilizan de conformidad con normas en materia de protección de la intimidad y de los datos, al tiempo que tratan datos que cumplen normas estrictas en términos de calidad e integridad. Por «transparencia» se entiende que los sistemas de IA se desarrollan y utilizan de un modo que permita una trazabilidad y explicabilidad adecuadas, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA e informe debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos. Por «diversidad, no discriminación y equidad» se entiende que los sistemas de IA se desarrollan y utilizan de un modo que incluya a diversos agentes y promueve la igualdad de acceso, la igualdad de género y la diversidad cultural, al tiempo que se evitan los efectos discriminatorios y los sesgos injustos prohibidos por el Derecho nacional o de la Unión. Por «bienestar social y ambiental» se entiende que los sistemas de IA se desarrollan y utilizan de manera sostenible y respetuosa con el medio ambiente, así como en beneficio de todos los seres humanos, al tiempo que se supervisan y evalúan los efectos a largo plazo en las personas, la sociedad y la democracia. La aplicación de esos principios debe traducirse, cuando sea posible, en el diseño y el uso de modelos de IA. En cualquier caso, deben servir de base para la elaboración de códigos de conducta en virtud del presente Reglamento. Se anima a todas las partes interesadas, incluidos la industria, el mundo académico, la sociedad civil y las organizaciones de normalización, a que tengan en cuenta, según proceda, los principios éticos para el desarrollo de normas y mejores prácticas voluntarias.

(28) Al margen de los múltiples usos beneficiosos de la IA, esta 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 e incorrectas y deben estar prohibidas, pues van en contra de los valores de la Unión de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y de los derechos fundamentales consagrados en la Carta, como el derecho a la no discriminación, a la protección de datos y a la intimidad y los derechos del niño.

(29) Las técnicas de manipulación que posibilita la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente. Son especialmente peligrosos y, por tanto, deben prohibirse la introducción en el mercado, la puesta en servicio o la utilización de determinados sistemas de IA con el objetivo o al efecto de alterar de manera sustancial el comportamiento humano, con la consiguiente probabilidad de que se produzcan perjuicios considerables, en particular perjuicios con efectos adversos suficientemente importantes en la salud física o mental o en los intereses financieros. Esos sistemas de IA utilizan componentes subliminales, como estímulos de audio, imagen o vídeo que las personas no pueden percibir —ya que dichos estímulos trascienden la percepción humana—, u otras técnicas manipulativas o engañosas que socavan o perjudican la autonomía, la toma de decisiones o la capacidad de elegir libremente de las personas de maneras de las que estas no son realmente conscientes de dichas técnicas o, cuando lo son, pueden seguir siendo engañadas o no pueden controlarlas u oponerles resistencia. Esto podría facilitarse, por ejemplo, mediante interfaces cerebro-máquina o realidad virtual, dado que permiten un mayor grado de control acerca de qué estímulos se presentan a las personas, en la medida en que pueden alterar sustancialmente su comportamiento de un modo que suponga un perjuicio considerable. Además, los sistemas de IA también pueden explotar de otras maneras las vulnerabilidades de una persona o un colectivo específico de personas derivadas de su edad, su discapacidad en el sentido de lo dispuesto en la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo ([16]) o de una situación social o económica concreta que probablemente aumente su vulnerabilidad a la explotación, como vivir en condiciones de pobreza extrema o pertenecer a minorías étnicas o religiosas. Estos sistemas de IA pueden introducirse en el mercado, ponerse en servicio o utilizarse con el objetivo de alterar de manera sustancial el comportamiento de una persona, o tener ese efecto, y de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra persona o colectivo de personas, incluidos perjuicios que pueden acumularse a lo largo del tiempo y que, por tanto, deben prohibirse. No puede presuponerse que existe

([16]) Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios (DO L 151 de 7.6.2019, p. 70).

la intención de alterar el comportamiento si la alteración es el resultado de factores externos al sistema de IA que escapan al control del proveedor o del responsable del despliegue, a saber, factores que no es lógico prever y que, por tanto, el proveedor o el responsable del despliegue del sistema de IA no pueden mitigar. En cualquier caso, no es necesario que el proveedor o el responsable del despliegue tengan la intención de causar un perjuicio considerable, siempre que dicho perjuicio se derive de las prácticas de manipulación o explotación que posibilita la IA. La prohibición de tales prácticas de IA complementa lo dispuesto en la Directiva 2005/29/CE del Parlamento Europeo y del Consejo ([17]), en particular la prohibición, en cualquier circunstancia, de las prácticas comerciales desleales que causan perjuicios económicos o financieros a los consumidores, hayan sido establecidas mediante de sistemas de IA o de otra manera. La prohibición de las prácticas de manipulación y explotación establecida en el presente Reglamento no debe afectar a prácticas lícitas en el contexto de un tratamiento médico, como el tratamiento psicológico de una enfermedad mental o la rehabilitación física, cuando dichas prácticas se lleven a cabo de conformidad con el Derecho y las normas médicas aplicables, por ejemplo, con el consentimiento expreso de las personas o de sus representantes legales. Asimismo, no debe considerarse que las prácticas comerciales comunes y legítimas (por ejemplo, en el campo de la publicidad) que cumplan el Derecho aplicable son, en sí mismas, prácticas de manipulación perjudiciales que posibilita la IA.

(30) Deben prohibirse los sistemas de categorización biométrica basados en datos biométricos de las personas físicas, como la cara o las impresiones dactilares de una persona física, para deducir o inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona física. Dicha prohibición no debe aplicarse al etiquetado, al filtrado ni a la categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho nacional o de la Unión en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o del color de ojos, que pueden utilizarse, por ejemplo, en el ámbito de la garantía del cumplimiento del Derecho.

(31) Los sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas pueden tener resultados discriminatorios y abocar a la exclusión a determinados colectivos. Pueden menoscabar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia. Dichos sistemas de IA evalúan o clasifican a las personas físicas o a grupos de estas sobre la base de varios puntos de datos relacionados con su comportamiento social en múltiples contextos o de características personales o de su personalidad conocidas, inferidas o predichas durante determinados períodos de tiempo. La puntuación ciudadana resultante de dichos sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de determinadas 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, deben prohibirse los sistemas de IA que impliquen esas prácticas inaceptables de puntuación y den lugar a esos resultados perjudiciales o desfavorables. Esa prohibición no debe afectar a prácticas lícitas de evaluación de las personas físicas que se efectúen para un fin específico de conformidad con el Derecho de la Unión y nacional.

(32) 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 garantía del cumplimiento del Derecho invade de forma especialmente grave 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. 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 efectos discriminatorios. Tales posibles resultados sesgados y efectos discriminatorios son especialmente pertinentes por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. 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 que estos conllevan para los derechos y las libertades de las personas afectadas en el contexto de actividades de garantía del cumplimiento del Derecho, o afectadas por estas.

(33) En consecuencia, debe prohibirse el uso de dichos sistemas con fines de garantía del cumplimiento del Derecho, salvo en situaciones enumeradas de manera limitativa y definidas con precisión en las que su utilización sea estrictamente necesaria para lograr un interés público esencial cuya importancia compense los riesgos. Esas situaciones son la búsqueda de determinadas víctimas de un delito, incluidas personas desaparecidas; determinadas amenazas para la vida o para la seguridad física de las personas físicas o amenazas de atentado terrorista; y la localización o identificación de los autores o sospechosos de los delitos enumerados en un anexo del presente Reglamento, cuando dichas infracciones se castiguen en el Estado miembro de que se trate con una pena o una

([17]) Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales») (DO L 149 de 11.6.2005, p. 22).

medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años, y 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 la infracción sea lo suficientemente grave como para llegar a justificar el uso de sistemas de identificación biométrica remota «en tiempo real». Por otro lado, la lista de delitos proporcionada en un anexo del presente Reglamento se basa en los treinta y dos delitos enumerados en la Decisión Marco 2002/584/JAI del Consejo ([18]), si bien es preciso tener en cuenta que, en la práctica, es probable que algunas sean más relevantes que otras en el sentido de que es previsible que recurrir a la identificación biométrica remota «en tiempo real» podría ser necesario y proporcionado en grados muy distintos para llevar a cabo la localización o la identificación de los autores o sospechosos de las distintas infracciones enumeradas, y que es probable que haya diferencias en la gravedad, la probabilidad y la magnitud de los perjuicios o las posibles consecuencias negativas. Una amenaza inminente para la vida o la seguridad física de las personas físicas también podría derivarse de una perturbación grave de infraestructuras críticas, tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo ([19]), cuando la perturbación o destrucción de dichas infraestructuras críticas suponga una amenaza inminente para la vida o la seguridad física de una persona, también al perjudicar gravemente el suministro de productos básicos a la población o el ejercicio de la función esencial del Estado. Además, el presente Reglamento debe preservar la capacidad de las autoridades garantes del cumplimiento del Derecho, de control fronterizo, de la inmigración o del asilo para llevar a cabo controles de identidad en presencia de la persona afectada, de conformidad con las condiciones establecidas en el Derecho de la Unión y en el Derecho nacional para estos controles. En particular, las autoridades garantes del cumplimiento del Derecho, del control fronterizo, de la inmigración o del asilo deben poder utilizar sistemas de información, de conformidad con el Derecho de la Unión o el Derecho nacional, para identificar a las personas que, durante un control de identidad, se nieguen a ser identificadas o no puedan declarar o demostrar su identidad, sin que el presente Reglamento exija que se obtenga una autorización previa. Puede tratarse, por ejemplo, de una persona implicada en un delito que no quiera revelar su identidad a las autoridades garantes del cumplimiento del Derecho, o que no pueda hacerlo debido a un accidente o a una afección médica.

(34) Para velar por que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en esas situaciones enumeradas de manera limitativa y definidas con precisión, se tengan en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que dé lugar a la solicitud, a las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas, y a las garantías 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 garantía del cumplimiento del Derecho debe llevarse a cabo únicamente para confirmar la identidad de la persona que constituya el objetivo específico y limitarse a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal, teniendo en cuenta, en particular, las pruebas o indicios relativos a las amenazas, las víctimas o los autores. El uso del sistema de identificación biométrica remota en tiempo real en espacios de acceso público solo debe autorizarse si la correspondiente autoridad garante del cumplimiento del Derecho ha llevado a cabo una evaluación de impacto relativa a los derechos fundamentales y, salvo que se disponga otra cosa en el presente Reglamento, si ha registrado el sistema en la base de datos establecida en el presente Reglamento. La base de datos de personas de referencia debe ser adecuada para cada supuesto de uso en cada una de las situaciones antes mencionadas.

(35) Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho debe haber sido autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro y cuya decisión sea vinculante. En principio, dicha autorización debe obtenerse antes de utilizar el sistema de IA con el fin de identificar a una o varias personas. Deben permitirse excepciones a esa norma en situaciones debidamente justificadas por motivos de urgencia, a saber, en aquellas en las que la necesidad de utilizar los sistemas de que se trate sea tan imperiosa que resulte efectiva y objetivamente imposible obtener una autorización antes de iniciar el uso del sistema de IA. En tales situaciones de urgencia, el uso debe limitarse al mínimo imprescindible y satisfacer las garantías y condiciones oportunas, conforme a lo dispuesto en el Derecho nacional y según corresponda en cada supuesto concreto de uso urgente por parte de la propia autoridad garante del cumplimiento del Derecho. Además, en esas situaciones las autoridades garantes del cumplimiento del Derecho deben solicitar dicha autorización e indicar los motivos por los que no han podido hacerlo antes, sin demora indebida y, como máximo, en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso de sistemas de identificación biométrica en tiempo real vinculados a la autorización debe interrumpirse con efecto inmediato y todos los datos relacionados con dicho uso deben desecharse y suprimirse. Entre esos datos se incluyen los datos de entrada directamente adquiridos por un sistema de IA durante el uso de dicho sistema, así como los resultados y la información de salida del uso vinculados a dicha autorización. No debe incluir la información de entrada adquirida legalmente de conformidad con otro acto del Derecho nacional o de la Unión. En cualquier caso, no debe adoptarse ninguna decisión que produzca efectos

([18]) 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).

([19]) Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164).

jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota.

(36) A fin de desempeñar sus funciones de conformidad con los requisitos establecidos en el presente Reglamento, así como en las normas nacionales, debe notificarse a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos cada uso del sistema de identificación biométrica en tiempo real. Las autoridades de vigilancia del mercado y las autoridades nacionales de protección de datos que hayan recibido una notificación deben presentar a la Comisión un informe anual sobre el uso de sistemas de identificación biométrica en tiempo real.

(37) Por otro lado, conviene disponer, 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 de que se trate haya decidido contemplar expresamente la posibilidad de autorizarlo en las normas detalladas de su Derecho nacional, y en la medida en que lo haya contemplado. En consecuencia, con arreglo al presente Reglamento los Estados miembros siguen teniendo la libertad 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. Dichas normas nacionales deben notificarse a la Comisión en un plazo de treinta días a partir de su adopción.

(38) 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 garantía del cumplimiento del Derecho 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 correspondientes datos biométricos. Por lo tanto, ese uso y tratamiento deben ser posibles únicamente en la medida en que sean compatibles con el marco establecido por el presente Reglamento, sin que haya margen, fuera de dicho marco, para que las autoridades competentes, cuando actúen con fines de garantía del cumplimiento del Derecho, utilicen tales sistemas y traten dichos datos en los supuestos previstos en el artículo 10 de la Directiva (UE) 2016/680. En ese sentido, el presente Reglamento no tiene por objeto proporcionar 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 garantía del cumplimiento del Derecho, también por parte de las autoridades competentes, no debe estar sujeto al marco específico establecido por el presente Reglamento en lo que respecta al uso de dichos sistemas con fines de garantía del cumplimiento del Derecho. Por consiguiente, su uso con fines distintos de la garantía del cumplimiento del Derecho no debe estar sujeto al requisito de obtener una autorización previsto en el presente Reglamento ni a las normas de desarrollo aplicables del Derecho nacional que puedan hacer efectiva dicha autorización.

(39) Todo tratamiento de datos biométricos y de datos personales de otra índole asociado al uso de sistemas de IA para la identificación biométrica, salvo el asociado al uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho regulado por el presente Reglamento, debe seguir cumpliendo todos los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680. El artículo 9, apartado 1, del Reglamento (UE) 2016/679 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 prohíben el tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho, con las excepciones limitadas previstas en dichos artículos. En la aplicación del artículo 9, apartado 1, del Reglamento (UE) 2016/679, el uso de la identificación biométrica remota para fines distintos de la garantía del cumplimiento del Derecho ya ha sido objeto de decisiones de prohibición por parte de las autoridades nacionales de protección de datos.

(40) 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, las normas establecidas en el artículo 5, apartado 1, párrafo primero, letra g), en la medida en que se aplica al uso de sistemas de categorización biométrica para actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal, el artículo 5, apartado 1, párrafo primero, letra d), en la medida en que se aplica al uso de sistemas de IA comprendidos en el ámbito de aplicación de dicho artículo, el artículo 5, apartado 1, párrafo primero, letra h), y apartados 2 a 6, y el artículo 26, apartado 10, del presente Reglamento, adoptadas basándose en el artículo 16 del TFUE que se refieran al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, de dicho Tratado solo serán vinculantes para Irlanda en la medida en que sean vinculantes para este Estado normas de la Unión que regulen formas de cooperación judicial en materia penal y de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas basándose en el artículo 16 del TFUE.

(41) 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, las normas establecidas en el artículo 5, apartado 1, párrafo primero, letra g), en la medida en que se aplica al uso de sistemas de categorización biométrica para actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal, el artículo 5, apartado 1, párrafo primero, letra d), en la medida en que se aplican al uso de sistemas de IA comprendidos en el ámbito de aplicación de dicho artículo, el artículo 5,

apartado 1, párrafo primero, letra h), y apartados 2 a 6, y el artículo 26, apartado 10, del presente Reglamento, adoptadas sobre la base del artículo 16 del TFUE que se refieran al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, de dicho Tratado, no vincularán a Dinamarca ni le serán aplicables.

(42) En consonancia con la presunción de inocencia, las personas físicas de la Unión siempre deben ser juzgadas basándose en su comportamiento real. Las personas físicas nunca deben ser juzgadas a partir de comportamientos predichos por una IA basados únicamente en la elaboración de sus perfiles, en los rasgos o características de su personalidad, como la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de vehículo, sin una valoración humana y sin que exista una sospecha razonable, basada en hechos objetivos comprobables, de que dicha persona está implicada en una actividad delictiva. Por lo tanto, deben prohibirse las evaluaciones de riesgos realizadas con respecto a personas físicas para evaluar la probabilidad de que cometan un delito o para predecir la comisión de un delito real o potencial basándose únicamente en la elaboración de perfiles de esas personas físicas o la evaluación de los rasgos y características de su personalidad. En cualquier caso, dicha prohibición no se refiere o atañe a los análisis de riesgos que no estén basados en la elaboración de perfiles de personas o en los rasgos y características de la personalidad de las personas, como los sistemas de IA que utilizan los análisis de riesgos para evaluar la probabilidad de fraude financiero por parte de empresas sobre la base de transacciones sospechosas o las herramientas de análisis de riesgo para predecir la probabilidad de localización de estupefacientes y mercancías ilícitas por parte de las autoridades aduaneras, por ejemplo basándose en las rutas de tráfico conocidas.

(43) La introducción en el mercado, la puesta en servicio para ese fin concreto o la utilización de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir de internet o de imágenes de circuito cerrado de televisión deben estar prohibidas, pues esas prácticas agravan el sentimiento de vigilancia masiva y pueden dar lugar a graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad.

(44) Existe una gran preocupación respecto a la base científica de los sistemas de IA que procuran detectar o deducir las emociones, especialmente porque la expresión de las emociones varía de forma considerable entre culturas y situaciones, e incluso en una misma persona. Algunas de las deficiencias principales de estos sistemas son la fiabilidad limitada, la falta de especificidad y la limitada posibilidad de generalizar. Por consiguiente, los sistemas de IA que detectan o deducen las emociones o las intenciones de las personas físicas a partir de sus datos biométricos pueden tener resultados discriminatorios y pueden invadir los derechos y las libertades de las personas afectadas. Teniendo en cuenta el desequilibrio de poder en el contexto laboral o educativo, unido al carácter intrusivo de estos sistemas, dichos sistemas podrían dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o colectivos enteros. Por tanto, debe prohibirse la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA destinados a ser utilizados para detectar el estado emocional de las personas en situaciones relacionadas con el lugar de trabajo y el ámbito educativo. Dicha prohibición no debe aplicarse a los sistemas de IA introducidos en el mercado estrictamente con fines médicos o de seguridad, como los sistemas destinados a un uso terapéutico.

(45) El presente Reglamento no debe afectar a las prácticas prohibidas por el Derecho de la Unión, incluido el Derecho de la Unión en materia de protección de datos, de no discriminación, de protección de los consumidores y sobre competencia.

(46) La introducción en el mercado de la Unión, la puesta en servicio o la utilización de sistemas de IA de alto riesgo 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 cuyos resultados de salida se utilicen en la Unión no planteen riesgos inaceptables para intereses públicos importantes de la Unión, reconocidos y protegidos por el Derecho de la Unión. Sobre la base del nuevo marco legislativo, tal como se aclara en la Comunicación de la Comisión titulada «"Guía azul" sobre la aplicación de la normativa europea relativa a los productos, de 2022» ([20]), la norma general es que más de un acto jurídico de la legislación de armonización de la Unión, como los Reglamentos (UE) 2017/745 ([21]) y (UE) 2017/746 ([22]) del Parlamento Europeo y del Consejo o la Directiva 2006/42/CE del Parlamento Europeo y del Consejo ([23]) puedan aplicarse a un producto, dado que la introducción en el mercado o la puesta en servicio solo pueden tener lugar cuando el producto cumple toda la legislación de armonización de la Unión aplicable. A fin de

([20]) DO C 247 de 29.6.2022, p. 1.

([21]) 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).

([22]) 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).

([23]) Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24).

garantizar la coherencia y evitar cargas administrativas o costes innecesarios, los proveedores de un producto que contenga uno o varios sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento y de la legislación de armonización de la Unión incluida en una lista de un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas relativas a la manera de garantizar la conformidad de un producto que contenga uno o varios sistemas de IA con todos los requisitos aplicables de la legislación de armonización de la Unión de manera óptima. La clasificación de un sistema de IA como «de alto riesgo» debe limitarse a aquellos sistemas de IA que tengan un efecto perjudicial considerable en la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación debe reducir al mínimo cualquier posible restricción del comercio internacional.

(47) Los sistemas de IA pueden tener un efecto adverso para la salud y la seguridad de las personas, en particular cuando funcionan como componentes de seguridad 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 de velar por que solo lleguen al mercado aquellos productos que sean seguros y conformes, es importante prevenir y mitigar 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 atención personal deben poder funcionar y desempeñar sus funciones de manera segura en entornos complejos. Del mismo modo, en el sector sanitario, donde puede haber repercusiones especialmente importantes en la vida y la salud, los sistemas de diagnóstico y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, deben ser fiables y precisos.

(48) La magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es especialmente importante a la hora de clasificar un sistema de IA 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, el derecho a la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración. Además de esos derechos, conviene poner de relieve el hecho de que los menores poseen unos derechos específicos consagrados en el artículo 24 de la Carta y en la Convención sobre los Derechos del Niño de las Naciones Unidas, que se desarrollan con más detalle en la observación general n.º 25 de la Convención sobre los Derechos del Niño de Naciones Unidas 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, también 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.

(49) En relación con 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 ([24]), el Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo ([25]), el Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo ([26]), la Directiva 2014/90/UE del Parlamento Europeo y del Consejo ([27]), la Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo ([28]), el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo ([29]), el Reglamento (UE) 2018/1139 del Parlamento Europeo y

([24]) 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).

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) 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 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).

del Consejo ([30]), y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo ([31]), procede modificar dichos actos para garantizar que, cuando la Comisión adopte actos delegados o de ejecución pertinentes basados 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 los mecanismos y las autoridades de gobernanza, evaluación de la conformidad y control del cumplimiento vigentes establecidos en dichos actos.

(50) 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 determinados actos legislativos de armonización de la Unión enumerados en un anexo del presente Reglamento, procede clasificarlos como de alto riesgo en virtud del presente Reglamento si el producto de que se trate es sometido a un procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad de terceros de acuerdo con dichos actos legislativos de armonización 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, equipos de embarcaciones de recreo, instalaciones de transporte por cable, aparatos que queman combustibles gaseosos, productos sanitarios, productos sanitarios para diagnóstico *in vitro*, automoción y aviación.

(51) Que un sistema de IA se clasifique como de alto riesgo en virtud del presente Reglamento no significa necesariamente que el producto del que sea componente de seguridad, o el propio sistema de IA como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la correspondiente legislación de armonización de la Unión que se aplique al producto. Tal es el caso, en particular, de los Reglamentos (UE) 2017/745 y (UE) 2017/746, que prevén una evaluación de la conformidad de terceros de los productos de riesgo medio y alto.

(52) En cuanto a los sistemas de IA independientes, a saber, aquellos sistemas de IA de alto riesgo que no son componentes de seguridad de productos, o que son productos en sí mismos, deben clasificarse como de alto riesgo si, a la luz de su finalidad prevista, presentan un alto riesgo de ser perjudiciales para 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 varios ámbitos predefinidos especificados 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, que la Comisión debe estar facultada para adoptar, mediante actos delegados, a fin de tener en cuenta el rápido ritmo del desarrollo tecnológico, así como los posibles cambios en el uso de los sistemas de IA.

(53) También es importante aclarar que pueden existir casos específicos en los que los sistemas de IA referidos en ámbitos predefinidos especificados en el presente Reglamento no entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por dichos ámbitos, dado que no influyen sustancialmente en la toma de decisiones o no perjudican dichos intereses sustancialmente. A efectos del presente Reglamento, por sistema de IA que no influye sustancialmente en el resultado de la toma de decisiones debe entenderse un sistema de IA que no afecta al fondo, ni por consiguiente al resultado, de la toma de decisiones, ya sea humana o automatizada. Un sistema de IA que no influye sustancialmente en el resultado de la toma de decisiones podría incluir situaciones en las que se cumplen una o varias de las siguientes condiciones. La primera de dichas condiciones debe ser que el sistema de IA esté destinado a realizar una tarea de procedimiento delimitada, como un sistema de IA que transforme datos no estructurados en datos estructurados, un sistema de IA que clasifique en categorías los documentos recibidos o un sistema de IA que se utilice para detectar duplicados entre un gran número de aplicaciones. La naturaleza de esas tareas es tan restringida y limitada que solo presentan riesgos limitados que no aumentan por la utilización de un sistema de IA en un contexto que un anexo al presente Reglamento recoja como uso de alto riesgo. La segunda condición debe ser que la tarea realizada por el sistema de IA esté destinada a mejorar el resultado de una actividad

([30]) 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 y (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).

([31]) 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 de 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).

previa llevada a cabo por un ser humano, que pudiera ser pertinente a efectos de las utilizaciones de alto riesgo enumeradas en un anexo del presente Reglamento. Teniendo en cuenta esas características, el sistema de IA solo añade un nivel adicional a la actividad humana, entrañando por consiguiente un riesgo menor. Esa condición se aplicaría, por ejemplo, a los sistemas de IA destinados a mejorar el lenguaje utilizado en documentos ya redactados, por ejemplo, en lo referente al empleo de un tono profesional o de un registro lingüístico académico o a la adaptación del texto a una determinada comunicación de marca. La tercera condición debe ser que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones respecto de patrones de toma de decisiones anteriores. El riesgo sería menor debido a que el sistema de IA se utiliza tras una valoración humana previamente realizada y no pretende sustituirla o influir en ella sin una revisión adecuada por parte de un ser humano. Por ejemplo, entre los sistemas de IA de este tipo, se incluyen aquellos que pueden utilizarse para comprobar *a posteriori* si un profesor puede haberse desviado de su patrón de calificación determinado, a fin de llamar la atención sobre posibles incoherencias o anomalías. La cuarta condición debe ser que el sistema de IA esté destinado a realizar una tarea que solo sea preparatoria de cara a una evaluación pertinente a efectos de los sistemas de IA enumerados en el anexo del presente Reglamento, con lo que la posible repercusión de los resultados de salida del sistema sería muy escasa en términos de representar un riesgo para la subsiguiente evaluación. Esa condición comprende, entre otras cosas, soluciones inteligentes para la gestión de archivos, lo que incluye funciones diversas tales como la indexación, la búsqueda, el tratamiento de texto y del habla o la vinculación de datos a otras fuentes de datos, o bien los sistemas de IA utilizados para la traducción de los documentos iniciales. En cualquier caso, debe considerarse que los sistemas de IA utilizados en casos de alto riesgo enumerados en un anexo del presente Reglamento presentan un riesgo significativo de menoscabar la salud y la seguridad o los derechos fundamentales si el sistema de IA conlleva la elaboración de perfiles en el sentido del artículo 4, punto 4, del Reglamento (UE) 2016/679, del artículo 3, punto 4, de la Directiva (UE) 2016/680 o del artículo 3, punto 5, del Reglamento (UE) 2018/1725. Para garantizar la trazabilidad y la transparencia, los proveedores que, basándose en las condiciones antes citadas, consideren que un sistema de IA no es de alto riesgo, deben elaborar la documentación de la evaluación previamente a la introducción en el mercado o la entrada en servicio de dicho sistema de IA y facilitarla a las autoridades nacionales competentes cuando estas lo soliciten. Dichos proveedores deben tener la obligación de registrar el sistema en la base de datos de la UE creada en virtud del presente Reglamento. Con el fin de proporcionar orientaciones adicionales sobre la aplicación práctica de las condiciones con arreglo a las cuales los sistemas de IA enumerados en un anexo del presente Reglamento no se consideran, con carácter excepcional, de alto riesgo, la Comisión debe, previa consulta al Consejo de IA, proporcionar directrices que especifiquen dicha aplicación práctica, completadas por una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y de casos de uso que no lo sean.

(54) Dado que los datos biométricos constituyen una categoría de datos personales sensibles, procede clasificar como de alto riesgo varios casos de uso críticos de sistemas biométricos, en la medida que su utilización esté permitida con arreglo al Derecho de la Unión y nacional pertinente. 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 efectos discriminatorios. El riesgo de dichos resultados sesgados y efectos discriminatorios es especialmente pertinente por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Por lo tanto, los sistemas de identificación biométrica remota deben clasificarse como de alto riesgo debido a los riesgos que entrañan. Quedan excluidos de dicha clasificación los sistemas de IA destinados a la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física concreta es quien dicha persona dice ser, así como confirmar la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga un acceso seguro a un local. Además, deben clasificarse como de alto riesgo los sistemas de IA destinados a ser utilizados para la categorización biométrica conforme a atributos o características sensibles protegidos en virtud del artículo 9, apartado 1, del Reglamento (UE) 2016/679 sobre la base de datos biométricos, en la medida en que no estén prohibidos en virtud del presente Reglamento, así como los sistemas de reconocimiento de emociones que no estén prohibidos con arreglo al presente Reglamento. Los sistemas biométricos destinados a ser utilizados exclusivamente a efectos de posibilitar la ciberseguridad y las medidas de protección de los datos personales no deben considerarse sistemas de IA de alto riesgo.

(55) Por lo que respecta a la gestión y el funcionamiento de infraestructuras críticas, procede clasificar como de alto riesgo los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas que se enumeran en el anexo, punto 8, de la Directiva (UE) 2022/2557; del tráfico rodado y del suministro de agua, gas, calefacción y electricidad, pues un fallo o un defecto de funcionamiento de estos componentes puede poner en peligro la vida y la salud de las personas a gran escala y alterar de manera considerable el desarrollo habitual de las actividades sociales y económicas. Los componentes de seguridad de las infraestructuras críticas, como las infraestructuras digitales críticas, son sistemas utilizados para proteger directamente la integridad física de las infraestructuras críticas o la salud y la seguridad de las personas y los bienes, pero que no son necesarios para el funcionamiento del sistema. El fallo o el defecto de

funcionamiento de estos componentes podría dar lugar directamente a riesgos para la integridad física de las infraestructuras críticas y, por tanto, a riesgos para la salud y la seguridad de las personas y los bienes. Los componentes destinados a ser utilizados exclusivamente con fines de ciberseguridad no deben considerarse componentes de seguridad. Entre los componentes de seguridad de esas infraestructuras críticas cabe citar los sistemas de control de la presión del agua o los sistemas de control de las alarmas contra incendios en los centros de computación en la nube.

(56) El despliegue de sistemas de IA en el ámbito educativo es importante para fomentar una educación y formación digitales de alta calidad y para que todos los estudiantes y profesores puedan adquirir y compartir las capacidades y competencias digitales necesarias, incluidos la alfabetización mediática, y el pensamiento crítico, para participar activamente en la economía, la sociedad y los procesos democráticos. No obstante, deben clasificarse como de alto riesgo los sistemas de IA que se utilizan en la educación o la formación profesional, y en particular aquellos que determinan el acceso o la admisión, distribuyen a las personas entre distintas instituciones educativas y de formación profesional o programas de todos los niveles, evalúan los resultados del aprendizaje de las personas, evalúan el nivel apropiado de educación de una persona e influyen sustancialmente en el nivel de educación y formación que las personas recibirán o al que podrán acceder, o supervisan y detectan comportamientos prohibidos de los estudiantes durante las pruebas, ya que pueden decidir la trayectoria formativa y profesional de una persona y, en consecuencia, puede afectar a su capacidad para asegurar su subsistencia. Cuando no se diseñan y utilizan correctamente, estos sistemas pueden invadir especialmente y violar el derecho a la educación y la formación, y el derecho a no sufrir discriminación, además de perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, las personas con discapacidad o las personas de cierto origen racial o étnico o con una determinada orientación sexual.

(57) También deben clasificarse como de alto riesgo los sistemas de IA que se utilizan en los ámbitos del empleo, la gestión de los trabajadores y el acceso al autoempleo, en particular para la contratación y la selección de personal, para la toma de decisiones que afecten a las condiciones de las relaciones de índole laboral, la promoción y la rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales y para la supervisión o evaluación de las personas en el marco de las relaciones contractuales de índole laboral, dado que pueden afectar de un modo considerable a las futuras perspectivas laborales, a los medios de subsistencia de dichas personas y a los derechos de los trabajadores. Las relaciones contractuales de índole laboral deben incluir, de manera significativa, a los empleados y las personas que prestan servicios a través de plataformas, como indica el programa de trabajo de la Comisión para 2021. Dichos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, las personas con discapacidad o las personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, promoción o retención de personas en las relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden socavar sus derechos fundamentales a la protección de los datos personales y a la intimidad.

(58) El acceso a determinados servicios y prestaciones esenciales, de carácter público y privado, necesarios para que las personas puedan participar plenamente en la sociedad o mejorar su nivel de vida, y el disfrute de dichos servicios y prestaciones, es otro ámbito en el que conviene prestar especial atención a la utilización de sistemas de IA. En particular, las personas físicas que solicitan a las autoridades públicas o reciben de estas prestaciones y servicios esenciales de asistencia pública, a saber, servicios de asistencia sanitaria, prestaciones de seguridad social, servicios sociales que garantizan una protección en casos como la maternidad, la enfermedad, los accidentes laborales, la dependencia o la vejez y la pérdida de empleo, asistencia social y ayudas a la vivienda, suelen depender de dichas prestaciones y servicios y, por lo general, se encuentran en una posición de vulnerabilidad respecto de las autoridades responsables. La utilización de sistemas de IA para decidir si las autoridades deben conceder, denegar, reducir o revocar dichas prestaciones y servicios o reclamar su devolución, lo que incluye decidir, por ejemplo, si los beneficiarios tienen legítimamente derecho a dichas prestaciones y servicios, podría tener un efecto considerable en los medios de subsistencia de las personas y vulnerar sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a la tutela judicial efectiva y, por lo tanto, deben clasificarse como de alto riesgo. No obstante, el presente Reglamento no debe obstaculizar el desarrollo y el uso de enfoques innovadores en la Administración, que podrían beneficiarse de una mayor utilización de sistemas de IA conformes y seguros, siempre y cuando dichos sistemas no supongan un alto riesgo para las personas jurídicas y físicas. Además, deben clasificarse como de alto riesgo los sistemas de IA usados para evaluar la calificación crediticia o solvencia de las 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 esos fines pueden discriminar a determinadas personas o colectivos y perpetuar patrones históricos de discriminación, como por motivos de origen racial o étnico, género, discapacidad, edad u orientación sexual, o generar nuevas formas de discriminación. No obstante, los sistemas de IA previstos por el Derecho de la Unión con vistas a detectar fraudes en la oferta de servicios financieros y, a efectos prudenciales, para calcular los requisitos de capital de las entidades de crédito y las empresas de seguros no deben considerarse de alto riesgo en virtud del presente Reglamento. Además, los sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las

personas físicas en el caso de los seguros de vida y de salud también pueden afectar de un modo considerable a los medios de subsistencia de las personas y, si no se diseñan, desarrollan y utilizan debidamente, pueden vulnerar sus derechos fundamentales y pueden tener graves consecuencias para la vida y la salud de las personas, como la exclusión financiera y la discriminación. Por último, los sistemas de IA empleados para evaluar y clasificar llamadas de emergencia de personas físicas o el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, incluidos policía, bomberos y servicios de asistencia médica, así como sistemas de triaje de pacientes para la asistencia sanitaria 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.

(59) Dado su papel y su responsabilidad, las actuaciones de las autoridades garantes del cumplimiento del Derecho que implican determinados usos de los 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 tener otros efectos negativos sobre los derechos fundamentales consagrados en la Carta. En particular, si el sistema de IA no está entrenado con datos de buena calidad, no cumple los requisitos adecuados en términos de rendimiento, de precisión o de solidez, o no se diseña y prueba debidamente antes de introducirlo en el mercado o ponerlo en servicio, es posible que señale 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 el derecho a la defensa y a la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén suficientemente bien documentados. Por consiguiente, en la medida en que su uso esté permitido conforme al Derecho de la Unión y nacional pertinente, procede clasificar como de alto riesgo varios sistemas de IA destinados a ser utilizados con fines de garantía del cumplimiento del Derecho 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 unas vías de recurso efectivas. En vista de la naturaleza de las actividades y de los riesgos conexos, entre dichos sistemas de IA de alto riesgo deben incluirse, en particular, los sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en nombre de estas, o por las instituciones, órganos u organismos de la Unión en apoyo de las primeras, para evaluar el riesgo de que una persona física sea víctima de delitos, como los polígrafos y otras herramientas similares, para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos y, en la medida en que no esté prohibido conforme al presente Reglamento, para evaluar el riesgo de que una persona física cometa un delito o reincida, no solo sobre la base de la elaboración de perfiles de personas físicas o la evaluación de rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o grupos de personas, o para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de delitos. Los sistemas de IA destinados específicamente a ser utilizados en procesos administrativos por las autoridades fiscales y aduaneras y las unidades de inteligencia financiera que desempeñan tareas administrativas de análisis de información de conformidad con el Derecho de la Unión en materia de lucha contra el blanqueo de capitales no deben clasificarse como sistemas de IA de alto riesgo usados por las autoridades garantes del cumplimiento del Derecho con el fin de prevenir, detectar, investigar y enjuiciar delitos. El uso de herramientas de IA por parte de las autoridades garantes del cumplimiento del Derecho y otras autoridades pertinentes no debe convertirse en un factor de desigualdad o exclusión. No debe ignorarse el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, en particular la dificultad para obtener información significativa sobre el funcionamiento de dichos sistemas y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas físicas investigadas.

(60) Los sistemas de IA empleados en la migración, el asilo y la gestión del control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y que dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilicen 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, su derecho a la libre circulación, a la no discriminación, a la intimidad personal y la protección de los datos personales, a la protección internacional y a una buena administración. Por lo tanto, procede clasificar como de alto riesgo, en la medida en que su utilización esté permitida en virtud del Derecho de la Unión y nacional, aquellos sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos u organismos de la Unión que realizan tareas en el ámbito de la migración, el asilo y la gestión del control fronterizo como polígrafos y herramientas similares, para evaluar determinados riesgos que presenten las personas físicas que entren en el territorio de un Estado miembro o que soliciten un visado o asilo, para ayudar a las autoridades públicas competentes a examinar, con inclusión de la evaluación conexa de la fiabilidad de las pruebas, 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 reúnen los requisitos necesarios para que se conceda su solicitud, a efectos de detectar, reconocer o identificar a las personas físicas en el contexto de la migración, el asilo y la gestión del control fronterizo, con excepción de la verificación de los documentos de viaje. Los sistemas de IA en el ámbito de la migración, el asilo y la gestión del control fronterizo sujetos al presente Reglamento deben cumplir los requisitos procedimentales pertinentes establecidos por el Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del

Consejo ([32]), la Directiva 2013/32/UE del Parlamento Europeo y del Consejo ([33]) y otro Derecho de la Unión pertinente. El empleo de los sistemas de IA en la migración, el asilo y la gestión del control fronterizo no debe, en ningún caso, ser utilizado por los Estados miembros o las instituciones, órganos u organismos de la Unión como medio para eludir sus obligaciones internacionales en virtud de la Convención de las Naciones Unidas sobre el Estatuto de los Refugiados, hecha en Ginebra el 28 de julio de 1951, modificada por el Protocolo de 31 de enero de 1967. Tampoco debe ser utilizado para infringir en modo alguno el principio de no devolución, ni para negar unas vías jurídicas seguras y efectivas de acceso al territorio de la Unión, incluido el derecho a la protección internacional.

(61) Deben clasificarse como de alto riesgo determinados 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 hacer frente al riesgo de posibles sesgos, errores y opacidades, procede clasificar como de alto riesgo aquellos sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. También deben considerarse de alto riesgo los sistemas de IA destinados a ser utilizados por los organismos de resolución alternativa de litigios con esos fines, cuando los resultados de los procedimientos de resolución alternativa de litigios surtan efectos jurídicos para las partes. La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe substituirlas: la toma de decisiones finales debe seguir siendo una actividad humana. No obstante, la clasificación de los sistemas de IA como de alto riesgo no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia propiamente dicha en casos concretos, como la anonimización o seudonimización de resoluciones judiciales, documentos o datos, la comunicación entre los miembros del personal o las tareas administrativas.

(62) Sin perjuicio de las normas previstas en el Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo ([34]), y a fin de hacer frente a los riesgos de injerencia externa indebida en el derecho de voto consagrado en el artículo 39 de la Carta, y de efectos adversos sobre la democracia y el Estado de Derecho, deben clasificarse como sistemas de IA de alto riesgo los sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o un referéndum, o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referendos, con excepción de los sistemas de IA a cuyos resultados de salida las personas físicas no están directamente expuestas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico.

(63) El hecho de que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea lícito con arreglo a otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión, por ejemplo, en materia de protección de los datos personales o 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 nacional. No debe entenderse que el presente Reglamento constituye un fundamento jurídico para el tratamiento de datos personales, incluidas las categorías especiales de datos personales, en su caso, salvo que el presente Reglamento disponga específicamente otra cosa.

(64) Con el objetivo de mitigar los riesgos que presentan los sistemas de IA de alto riesgo que se introducen en el mercado o se ponen en servicio, y para garantizar un alto nivel de fiabilidad, deben aplicarse a los sistemas de IA de alto riesgo ciertos requisitos obligatorios que tengan en cuenta la finalidad prevista y el contexto del uso del sistema de IA y estén en consonancia con el sistema de gestión de riesgos que debe establecer el proveedor. Las medidas adoptadas por los proveedores para cumplir los requisitos obligatorios del presente Reglamento deben tener en cuenta el estado actual de la técnica generalmente reconocido en materia de IA, ser proporcionadas y eficaces para alcanzar los objetivos del presente Reglamento. Sobre la base del nuevo marco legislativo, como se aclara en la Comunicación de la Comisión titulada «"Guía azul" sobre la aplicación de la normativa europea relativa a los productos, de 2022», la norma general es que más de un acto jurídico de la legislación de armonización de la Unión puede ser aplicable a un producto, ya que la comercialización o la puesta en servicio solamente puede producirse cuando el producto cumple toda la legislación de armonización de la Unión aplicable. Los peligros de los sistemas de IA cubiertos por los requisitos del presente Reglamento se refieren a aspectos diferentes de los contemplados en la legislación de armonización de la Unión existente y, por consiguiente, los requisitos del presente Reglamento completarían el conjunto existente de legislación de armonización de la Unión. Por ejemplo, las máquinas o los productos sanitarios que incorporan un sistema de IA pueden presentar riesgos de los que no se ocupan los

([32]) 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).

([33]) 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).

([34]) Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política (DO L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

requisitos esenciales de salud y seguridad establecidos en la legislación armonizada de la Unión pertinente, ya que esa legislación sectorial no aborda los riesgos específicos de los sistemas de IA. Esto exige una aplicación simultánea y complementaria de diversos actos legislativos. A fin de garantizar la coherencia y evitar una carga administrativa innecesaria y costes innecesarios, los proveedores de un producto que contenga uno o varios sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento y de los actos legislativos de armonización de la Unión basados en el nuevo marco legislativo y enumerados en un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas relativas a la manera de garantizar la conformidad de un producto que contenga uno o varios sistemas de IA con todos los requisitos aplicables de la legislación armonizada de la Unión de manera óptima. Esa flexibilidad podría significar, por ejemplo, la decisión del proveedor de integrar una parte de los procesos de prueba y notificación necesarios, así como la información y la documentación exigidas en virtud del presente Reglamento, en la documentación y los procedimientos ya existentes exigidos en virtud de los actos legislativos de armonización de la Unión vigentes basados en el nuevo marco legislativo y enumerados en un anexo del presente Reglamento. Esto no debe socavar en modo alguno la obligación del proveedor de cumplir todos los requisitos aplicables.

(65) El sistema de gestión de riesgos debe consistir en un proceso iterativo continuo que sea planificado y ejecutado durante todo el ciclo de vida del sistema de IA de alto riesgo. Dicho proceso debe tener por objeto detectar y mitigar los riesgos pertinentes de los sistemas de IA para la salud, la seguridad y los derechos fundamentales. El sistema de gestión de riesgos debe revisarse y actualizarse periódicamente para garantizar su eficacia continua, así como la justificación y documentación de cualesquiera decisiones y acciones significativas adoptadas con arreglo al presente Reglamento. Este proceso debe garantizar que el proveedor determine los riesgos o efectos negativos y aplique medidas de mitigación de los riesgos conocidos y razonablemente previsibles de los sistemas de IA para la salud, la seguridad y los derechos fundamentales, habida cuenta de su finalidad prevista y de su uso indebido razonablemente previsible, incluidos los posibles riesgos derivados de la interacción entre el sistema de IA y el entorno en el que opera. El sistema de gestión de riesgos debe adoptar las medidas de gestión de riesgos más adecuadas a la luz del estado actual de la técnica en materia de IA. Al determinar las medidas de gestión de riesgos más adecuadas, el proveedor debe documentar y explicar las elecciones realizadas y, cuando proceda, contar con la participación de expertos y partes interesadas externas. Al determinar el uso indebido razonablemente previsible de los sistemas de IA de alto riesgo, el proveedor debe tener en cuenta los usos de los sistemas de IA que, aunque no estén directamente cubiertos por la finalidad prevista ni establecidos en las instrucciones de uso, cabe esperar razonablemente que se deriven de un comportamiento humano fácilmente previsible en el contexto de las características específicas y del uso de un sistema de IA concreto. Debe incluirse en las instrucciones de uso que sean facilitadas por el proveedor 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. Con ello se pretende garantizar que el responsable del despliegue sea consciente de estos riesgos y los tenga en cuenta al utilizar el sistema de IA de alto riesgo. La identificación y la aplicación de medidas de reducción del riesgo en caso de uso indebido previsible con arreglo al presente Reglamento no deben suponer la exigencia, para su acometida, de entrenamiento adicional específico para el sistema de IA de alto riesgo por parte del proveedor para hacer frente a usos indebidos previsibles. No obstante, se anima a los proveedores a considerar dichas medidas de entrenamiento adicionales para mitigar los usos indebidos razonablemente previsibles, cuando resulte necesario y oportuno.

(66) Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la gestión de riesgos, la calidad y la pertinencia de los conjuntos de datos utilizados, la documentación técnica y la conservación de registros, la transparencia y la comunicación de información a los responsables del despliegue, la supervisión 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. Al no disponerse razonablemente de otras medidas menos restrictivas del comercio, dichos requisitos no son restricciones injustificadas al comercio.

(67) Los datos de alta calidad y el acceso a datos de alta calidad desempeñan un papel esencial a la hora de proporcionar una estructura y garantizar el funcionamiento de muchos sistemas de IA, en especial cuando se emplean técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funcione del modo previsto y en condiciones de seguridad y no se convierta en una fuente de algún tipo de discriminación prohibida por el Derecho de la Unión. Es preciso instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad. Los conjuntos de datos para el entrenamiento, la validación y la prueba, incluidas las etiquetas, deben ser pertinentes, lo suficientemente representativos y, en la mayor medida posible, estar libres de errores y ser completos en vista de la finalidad prevista del sistema. A fin de facilitar el cumplimiento del Derecho de la Unión en materia de protección de datos, como el Reglamento (UE) 2016/679, las prácticas de gestión y gobernanza de datos deben incluir, en el caso de los datos personales, la transparencia sobre el fin original de la recopilación de datos. Los conjuntos de datos deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los colectivos de personas en relación con los que esté previsto utilizar el sistema de IA de alto riesgo, prestando una atención especial a la mitigación de los posibles sesgos en los conjuntos de datos que puedan afectar a la salud y la seguridad de las personas físicas, tener repercusiones negativas en los derechos fundamentales o dar lugar a algún tipo de

discriminación prohibida por el Derecho de la Unión, especialmente cuando los datos de salida influyan en la información de entrada de futuras operaciones (bucles de retroalimentación). Los sesgos, por ejemplo, pueden ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, o generados cuando los sistemas se despliegan en entornos del mundo real. Los resultados de los sistemas de IA dependen de dichos sesgos inherentes, que tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados colectivos vulnerables, incluidos colectivos raciales o étnicos. El requisito de que los conjuntos de datos, en la mayor medida posible, sean completos y estén libres de errores no debe afectar al uso de técnicas de protección de la intimidad en el contexto del desarrollo y la prueba de sistemas de IA. En particular, los conjuntos de datos deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que esté previsto que se utilice el sistema de IA. Los requisitos relacionados con la gobernanza de datos pueden cumplirse recurriendo a terceros que ofrezcan servicios certificados de cumplimiento, incluida la verificación de la gobernanza de datos, la integridad del conjunto de datos y las prácticas de entrenamiento, validación y prueba de datos, en la medida en que se garantice el cumplimiento de los requisitos en materia de datos del presente Reglamento.

(68) Para poder desarrollar y evaluar sistemas de IA de alto riesgo, determinados agentes, tales como proveedores, organismos notificados y otras entidades pertinentes, como centros europeos de innovación digital, instalaciones de ensayo y experimentación e investigadores, deben tener acceso a conjuntos de datos de alta calidad en sus campos de actividad relacionados con el presente Reglamento y deben 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 favor 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 IA de una manera segura, oportuna, transparente, fiable y que respete la intimidad, y contando con la debida gobernanza institucional. Las autoridades competentes pertinentes, incluidas las sectoriales, que proporcionan acceso a datos o lo facilitan también pueden brindar apoyo al suministro de datos de alta calidad con los que entrenar, validar y probar los sistemas de IA.

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

(70) A fin de proteger los derechos de terceros frente a la discriminación que podría provocar el sesgo de los sistemas de IA, los proveedores deben —con carácter excepcional, en la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas y tras la aplicación de todas las condiciones aplicables establecidas en el presente Reglamento, además de las condiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680— ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial en el sentido del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y del artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725.

(71) Para permitir la trazabilidad de los sistemas de IA de alto riesgo, verificar si cumplen los requisitos previstos en el presente Reglamento, así como vigilar su funcionamiento y llevar a cabo la vigilancia poscomercialización, resulta esencial disponer de información comprensible sobre el modo en que se han desarrollado y sobre su funcionamiento durante toda su vida útil. A tal fin, es preciso llevar registros y disponer de documentación técnica que contenga la información necesaria para evaluar si el sistema de IA de que se trate cumple los requisitos pertinentes y facilitar la vigilancia poscomercialización. Dicha información debe incluir las características generales, las capacidades y las limitaciones del sistema y los algoritmos, datos y procesos de entrenamiento, prueba y validación empleados, así como documentación sobre el sistema de gestión de riesgos pertinente, elaborada de manera clara y completa. La documentación técnica debe mantenerse adecuadamente actualizada durante toda la vida útil del sistema de IA. Además, los sistemas de IA de alto riesgo deben permitir técnicamente el registro automático de acontecimientos, mediante archivos de registro, durante toda la vida útil del sistema.

(72) A fin de abordar las preocupaciones relacionadas con la opacidad y complejidad de determinados sistemas de IA y ayudar a los responsables del despliegue a cumplir sus obligaciones en virtud del presente Reglamento, debe exigirse transparencia respecto de los sistemas de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio. Los sistemas de IA de alto riesgo deben diseñarse de modo que permitan a los responsables del despliegue comprender la manera en que el sistema de IA funciona, evaluar su funcionalidad y comprender sus fortalezas y limitaciones. Los sistemas de IA de alto riesgo deben ir acompañados de la información adecuada en forma de instrucciones de uso. Dicha información debe incluir las características, las capacidades y las limitaciones del funcionamiento del sistema de IA. Estas comprenderían la información sobre las posibles circunstancias conocidas y previsibles relacionadas con el uso del sistema de IA de alto riesgo, incluida la actuación del responsable del despliegue capaz de influir en el comportamiento y el funcionamiento del sistema, en cuyo marco el sistema de IA puede dar lugar a riesgos para la salud, la seguridad y los derechos fundamentales, sobre los cambios que el proveedor haya predeterminado y evaluado para comprobar su conformidad y sobre las medidas pertinentes de supervisión humana, incluidas las medidas para facilitar la interpretación de los resultados de salida del sistema de IA por parte de los responsables del despliegue. La transparencia, incluidas las instrucciones de uso que acompañan a los sistemas de IA, debe ayudar a los responsables del despliegue a utilizar el sistema y tomar decisiones con conocimiento de causa. Los responsables del despliegue deben, entre otras cosas, estar en mejores condiciones para elegir correctamente el sistema que pretenden utilizar a la luz de las obligaciones que les son aplicables, estar informados sobre los usos previstos y excluidos y utilizar el sistema de IA correctamente y según proceda. A fin de mejorar la legibilidad y la accesibilidad de la información incluida en las instrucciones de uso, cuando proceda, deben incluirse ejemplos ilustrativos, por ejemplo sobre las limitaciones y sobre los usos previstos y excluidos del sistema de IA. Los proveedores deben garantizar que toda la documentación, incluidas las instrucciones de uso, contenga información significativa, exhaustiva, accesible y comprensible, que tenga en cuenta las necesidades y los conocimientos previsibles de los responsables del despliegue destinatarios. Las instrucciones de uso deben estar disponibles en una lengua fácilmente comprensible para los responsables del despliegue destinatarios, según lo que decida el Estado miembro de que se trate.

(73) Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que las personas físicas puedan supervisar su funcionamiento, así como asegurarse de que se usan según lo previsto y de que sus repercusiones se abordan a lo largo del ciclo de vida del sistema. A tal fin, el proveedor del sistema debe definir las medidas adecuadas de supervisión humana antes de su introducción en el mercado o puesta en servicio. Cuando proceda, dichas medidas deben garantizar, en concreto, que el sistema esté sujeto a limitaciones operativas incorporadas en el propio sistema que este no pueda desactivar, que responda al operador humano y que las personas físicas a quienes se haya encomendado la supervisión humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función. También es esencial, según proceda, garantizar que los sistemas de IA de alto riesgo incluyan mecanismos destinados a orientar e informar a las personas físicas a las que se haya asignado la supervisión humana para que tomen decisiones con conocimiento de causa acerca de si intervenir, cuándo hacerlo y de qué manera, a fin de evitar consecuencias negativas o riesgos, o de detener el sistema si no funciona según lo previsto. Teniendo en cuenta las enormes consecuencias para las personas en caso de una correspondencia incorrecta efectuada por determinados sistemas de identificación biométrica, conviene establecer un requisito de supervisión humana reforzada para dichos sistemas, de modo que el responsable del despliegue no pueda actuar ni tomar ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas la han verificado y confirmado por separado. Dichas personas podrían proceder de una o varias entidades e incluir a la persona que maneja o utiliza el sistema. Este requisito no debe suponer una carga ni retrasos innecesarios y podría bastar con que las verificaciones que las distintas personas efectúen por separado se registren automáticamente en los registros generados por el sistema. Dadas las especificidades de los ámbitos de la garantía del cumplimiento del Derecho, la migración, el control fronterizo y el asilo, ese requisito no debe aplicarse cuando el Derecho nacional o de la Unión considere que su aplicación es desproporcionada.

(74) Los sistemas de IA de alto riesgo deben funcionar de manera uniforme durante todo su ciclo de vida y presentar un nivel adecuado de precisión, solidez y ciberseguridad, a la luz de su finalidad prevista y con arreglo al estado actual de la técnica generalmente reconocido. Se anima a la Comisión y las organizaciones y partes interesadas pertinentes a que tengan debidamente en cuenta la mitigación de los riesgos y las repercusiones negativas del sistema de IA. El nivel previsto de los parámetros de funcionamiento debe declararse en las instrucciones de uso que acompañen a los sistemas de IA. Se insta a los proveedores a que comuniquen dicha información a los responsables del despliegue de manera clara y fácilmente comprensible, sin malentendidos ni afirmaciones engañosas. El Derecho de la Unión en materia de metrología legal, incluidas las Directivas 2014/31/UE ([35]) y 2014/32/UE ([36]) del Parlamento Europeo y del Consejo, tiene por objeto garantizar la precisión de las mediciones y contribuir a la transparencia y la equidad de las transacciones comerciales. En ese contexto, en cooperación con las partes interesadas y las organizaciones pertinentes, como las autoridades de metrología y de evaluación comparativa, la Comisión debe fomentar, según proceda, el desarrollo de parámetros de referencia y metodologías de medición para los sistemas de IA. Al hacerlo, la Comisión debe tomar nota de los socios internacionales que trabajan en la metrología y los indicadores de medición pertinentes relacionados con la IA y colaborar con ellos.

([35]) Directiva 2014/31/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de comercialización de instrumentos de pesaje de funcionamiento no automático (DO L 96 de 29.3.2014, p. 107).

([36]) Directiva 2014/32/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de comercialización de instrumentos de medida (DO L 96 de 29.3.2014, p. 149).

(75) La solidez técnica es un requisito clave para los sistemas de IA de alto riesgo, que deben ser resilientes en relación con los comportamientos perjudiciales o indeseables por otros motivos que puedan derivarse de limitaciones en los sistemas o del entorno en el que estos funcionan (p. ej., errores, fallos, incoherencias o situaciones inesperadas). Por consiguiente, deben adoptarse medidas técnicas y organizativas para garantizar la solidez de los sistemas de IA de alto riesgo, por ejemplo mediante el diseño y desarrollo de soluciones técnicas adecuadas para prevenir o reducir al mínimo ese comportamiento perjudicial o indeseable. Estas soluciones técnicas pueden incluir, por ejemplo, mecanismos que permitan al sistema interrumpir de forma segura su funcionamiento (planes de prevención contra fallos) en presencia de determinadas anomalías o cuando el funcionamiento tenga lugar fuera de determinados límites predeterminados. El hecho de no adoptar medidas de protección frente a estos riesgos podría tener consecuencias para la seguridad o afectar de manera negativa a los derechos fundamentales, por ejemplo, debido a decisiones equivocadas o resultados de salida erróneos o sesgados generados por el sistema de IA.

(76) 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, comportamiento o funcionamiento o de poner en peligro sus propiedades de seguridad. Los ciberataques contra sistemas de IA pueden dirigirse contra activos específicos de la IA, como los conjuntos de datos de entrenamiento (p. ej., envenenamiento de datos) o los modelos entrenados (p. ej., ataques adversarios o inferencia de pertenencia), o aprovechar las vulnerabilidades de los activos digitales del sistema de IA o la infraestructura de TIC subyacente. Por lo tanto, para garantizar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas, como los controles de seguridad, teniendo también en cuenta, cuando proceda, la infraestructura de TIC subyacente.

(77) Sin perjuicio de los requisitos relacionados con la solidez y la precisión establecidos en el presente Reglamento, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, de conformidad con dicho reglamento, pueden demostrar el cumplimiento con los requisitos de ciberseguridad del presente Reglamento mediante el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en dicho reglamento. Cuando los sistemas de IA de alto riesgo cumplan los requisitos esenciales de ciberseguridad de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, debe presumirse que cumplen los requisitos de ciberseguridad del presente Reglamento en la medida en que la satisfacción de esos requisitos se demuestre en la declaración UE de conformidad de emitida con arreglo a dicho reglamento, o partes de esta. A tal fin, la evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales clasificado como un sistema de IA de alto riesgo con arreglo al presente Reglamento, realizada en virtud de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, debe tener en cuenta los riesgos para la ciberresiliencia de un sistema de IA por lo que respecta a los intentos de terceros no autorizados de alterar su uso, comportamiento o funcionamiento, incluidas las vulnerabilidades específicas de la IA, como el envenenamiento de datos o los ataques adversarios, así como, en su caso, los riesgos para los derechos fundamentales, tal como exige el presente Reglamento.

(78) El procedimiento de evaluación de la conformidad establecido en el presente Reglamento debe aplicarse en relación con los requisitos esenciales de ciberseguridad de un producto con elementos digitales regulado por un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y clasificado como sistema de IA de alto riesgo con arreglo al presente Reglamento. Sin embargo, esta norma no debe dar lugar a una reducción del nivel de garantía necesario para los productos críticos con elementos digitales sujetos a un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales. Por consiguiente, no obstante lo dispuesto en esta norma, los sistemas de IA de alto riesgo que entran dentro del ámbito de aplicación del presente Reglamento y que también se consideran productos críticos importantes con elementos digitales en virtud de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, y a los que se aplica el procedimiento de evaluación de la conformidad fundamentado en un control interno que se establece en un anexo del presente Reglamento, están sujetos a lo dispuesto en un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales en materia de evaluación de la conformidad por lo que se refiere a los requisitos esenciales de ciberseguridad de dicho reglamento. En tal caso, en relación con todos los demás aspectos que entren en el ámbito de aplicación del presente Reglamento, debe aplicarse lo dispuesto en el anexo VI del presente Reglamento en materia de evaluación de la conformidad fundamentada en un control interno. Habida cuenta de los conocimientos y la experiencia de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en materia de política de ciberseguridad y de las tareas que se le encomiendan en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([37]), la Comisión debe cooperar con ENISA en las cuestiones relacionadas con la ciberseguridad de los sistemas de IA.

([37]) 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. 15).

(79) Conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad asociada a la introducción en el mercado o la 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.

(80) Como signatarios de la Convención sobre los Derechos de las Personas con Discapacidad, la Unión y todos los Estados miembros están legalmente obligados a proteger a las personas con discapacidad contra la discriminación y a promover su igualdad, a garantizar que las personas con discapacidad tengan acceso, en igualdad de condiciones con las demás, a las tecnologías y sistemas de la información y las comunicaciones, y a garantizar el respeto a la intimidad de las personas con discapacidad. Habida cuenta de la importancia y el uso crecientes de los sistemas de IA, la aplicación de los principios de diseño universal a todas las nuevas tecnologías y servicios debe garantizar el acceso pleno e igualitario de todas las personas a las que puedan afectar las tecnologías de IA o que puedan utilizar dichas tecnologías, incluidas las personas con discapacidad, de forma que se tenga plenamente en cuenta su dignidad y diversidad inherentes. Por ello es esencial que los proveedores garanticen el pleno cumplimiento de los requisitos de accesibilidad, incluidas la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo ([38]) y la Directiva (UE) 2019/882. Los proveedores deben garantizar el cumplimiento de estos requisitos desde el diseño. Por consiguiente, las medidas necesarias deben integrarse en la medida de lo posible en el diseño de los sistemas de IA de alto riesgo.

(81) 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 de vigilancia poscomercialización sólido. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad con arreglo al Derecho sectorial pertinente de la Unión deben tener la posibilidad de integrar los elementos del sistema de gestión de la calidad establecido en el presente Reglamento en el sistema de gestión de la calidad establecido en dicho Derecho sectorial de la Unión. La complementariedad entre el presente Reglamento y el Derecho sectorial vigente de la Unión también debe tenerse en cuenta en las futuras actividades de normalización o en las orientaciones adoptadas por la Comisión al respecto. 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 de que se trate.

(82) Para permitir la ejecución 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 la conformidad de un sistema de IA, teniendo en cuenta las distintas formas en que se pueden ofrecer productos digitales. Por lo tanto, antes de comercializar sus sistemas de IA en la Unión, los proveedores establecidos fuera de su territorio deben designar, mediante un mandato escrito, a un representante autorizado que se encuentre en la Unión. El representante autorizado desempeña un papel fundamental a la hora de velar por la conformidad de los sistemas de IA de alto riesgo introducidos en el mercado o puestos en servicio en la Unión por esos proveedores no establecidos en la Unión y servir de persona de contacto establecida en la Unión.

(83) Teniendo en cuenta la naturaleza y la complejidad de la cadena de valor de los sistemas de IA y de conformidad con el nuevo marco legislativo, es esencial garantizar la seguridad jurídica y facilitar el cumplimiento del presente Reglamento. Por ello es necesario aclarar la función y las obligaciones específicas de los operadores pertinentes de toda dicha cadena de valor, como los importadores y los distribuidores, que pueden contribuir al desarrollo de sistemas de IA. En determinadas situaciones, esos operadores pueden desempeñar más de una función al mismo tiempo y, por lo tanto, deben cumplir de forma acumulativa todas las obligaciones pertinentes asociadas a dichas funciones. Por ejemplo, un operador puede actuar como distribuidor e importador al mismo tiempo.

(84) Para garantizar la seguridad jurídica, es necesario aclarar que, en determinadas condiciones específicas, debe considerarse proveedor de un sistema de IA de alto riesgo a cualquier distribuidor, importador, responsable del despliegue u otro tercero que, por tanto, debe asumir todas las obligaciones pertinentes. Este sería el caso si, por ejemplo, esa persona pone su nombre o marca en un sistema de IA de alto riesgo ya introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen otra distribución de las obligaciones. Este también sería el caso si dicha parte modifica sustancialmente un sistema de IA de alto riesgo que ya se haya introducido en el mercado o puesto en servicio de tal manera que el sistema modificado siga siendo un sistema de IA de alto riesgo de conformidad con el presente Reglamento, o si modifica la finalidad prevista de un sistema de IA, como un sistema de IA de uso general, que ya se haya introducido en el mercado o puesto en servicio y que no esté clasificado como sistema de alto riesgo, de tal manera que el sistema modificado pase a ser un sistema de IA de alto riesgo de conformidad con el presente Reglamento. Esas disposiciones deben aplicarse sin perjuicio de las disposiciones más específicas establecidas en determinados actos legislativos de armonización de la Unión basados en el nuevo marco legislativo que se deben aplicar en conjunción con el presente Reglamento. Por ejemplo, el

([38]) Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público (DO L 327 de 2.12.2016, p. 1).

artículo 16, apartado 2, del Reglamento (UE) 2017/745, que establece que determinados cambios no deben considerarse modificaciones de un producto que puedan afectar al cumplimiento de los requisitos aplicables, debe seguir aplicándose a los sistemas de IA de alto riesgo que sean productos sanitarios en el sentido de dicho Reglamento.

(85) Los sistemas de IA de uso general pueden utilizarse como sistemas de IA de alto riesgo por sí solos o ser componentes de sistemas de IA de alto riesgo. Así pues, debido a su particular naturaleza y a fin de garantizar un reparto equitativo de responsabilidades a lo largo de toda la cadena de valor, los proveedores de tales sistemas, con independencia de que estos sistemas puedan ser utilizados como sistemas de IA de alto riesgo por sí solos por otros proveedores o como componentes de sistemas de IA de alto riesgo, y salvo que se disponga otra cosa en el presente Reglamento, deben cooperar estrechamente con los proveedores de los sistemas de IA de alto riesgo correspondientes para que estos puedan cumplir las obligaciones pertinentes en virtud del presente Reglamento, así como con las autoridades competentes establecidas en virtud del presente Reglamento.

(86) Cuando, con arreglo a las condiciones establecidas en el presente Reglamento, el proveedor que introdujo inicialmente el sistema de IA en el mercado o lo puso en servicio ya no deba considerarse el proveedor a los efectos del presente Reglamento, y cuando dicho proveedor no haya excluido expresamente la transformación del sistema de IA en un sistema de IA de alto riesgo, el primer proveedor debe, no obstante, cooperar estrechamente, facilitar la información necesaria y proporcionar el acceso técnico u otra asistencia que quepa esperar razonablemente y que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo.

(87) Además, cuando un sistema de IA de alto riesgo que sea un componente de seguridad de un producto que entre dentro del ámbito de aplicación de un acto legislativo de armonización de la Unión basado en el nuevo marco legislativo no se introduzca en el mercado ni se ponga en servicio de forma independiente del producto, el fabricante del producto, tal como se define en el acto legislativo pertinente, debe cumplir las obligaciones que el presente Reglamento impone al proveedor y, en particular, debe garantizar que el sistema de IA integrado en el producto final cumpla los requisitos del presente Reglamento.

(88) A lo largo de la cadena de valor de la IA, numerosas partes suministran a menudo no solo sistemas, herramientas y servicios de IA, sino también componentes o procesos que el proveedor incorpora al sistema de IA con diversos objetivos, como el entrenamiento de modelos, el reentrenamiento de modelos, la prueba y evaluación de modelos, la integración en el *software* u otros aspectos del desarrollo de modelos. Dichas partes desempeñan un papel importante en la cadena de valor en relación con el proveedor del sistema de IA de alto riesgo en el que se integran sus sistemas, herramientas, servicios, componentes o procesos de IA, y deben proporcionar a dicho proveedor, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y demás asistencia que sean necesarios habida cuenta del estado actual de la técnica generalmente reconocido, a fin de que el proveedor pueda cumplir íntegramente las obligaciones establecidas en el presente Reglamento, sin comprometer sus propios derechos de propiedad intelectual e industrial o secretos comerciales.

(89) A los terceros que ponen a disposición del público herramientas, servicios, procesos o componentes de IA que no sean modelos de IA de uso general no se les debe imponer la obligación de cumplir los requisitos relativos a las responsabilidades a lo largo de la cadena de valor de la IA, en particular por lo que respecta al proveedor que haya utilizado o integrado dichas herramientas, servicios, procesos o componentes de IA, cuando el acceso a dichas herramientas, servicios, procesos o componentes de IA esté sujeto a una licencia libre y de código abierto. No obstante, se debe animar a los desarrolladores de herramientas, servicios, procesos o componentes de IA libres y de código abierto que no sean modelos de IA de uso general a que apliquen prácticas de documentación ampliamente adoptadas, como tarjetas de modelo y hojas de datos, como una forma de acelerar el intercambio de información a lo largo de la cadena de valor de la IA, permitiendo la promoción en la Unión de sistemas de IA fiables.

(90) La Comisión podría elaborar y recomendar cláusulas contractuales tipo, de carácter voluntario, entre los proveedores de sistemas de IA de alto riesgo y los terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en los sistemas de IA de alto riesgo, a fin de facilitar la cooperación a lo largo de la cadena de valor. Cuando elabore estas cláusulas contractuales tipo de carácter voluntario, la Comisión también debe tener en cuenta los posibles requisitos contractuales aplicables en determinados sectores o modelos de negocio.

(91) Habida cuenta de las características de los sistemas de IA y de los riesgos que su uso lleva aparejado para la seguridad y los derechos fundamentales, también en lo que respecta a la necesidad de garantizar la correcta vigilancia del funcionamiento de un sistema de IA en un entorno real, conviene establecer las responsabilidades específicas de los responsables del despliegue. En particular, los responsables del despliegue deben adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas de IA de alto riesgo 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 la conservación de registros, según proceda. Asimismo, los responsables del despliegue deben garantizar que las personas encargadas de poner en práctica las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento tengan las competencias necesarias, en particular un nivel adecuado de alfabetización,

formación y autoridad en materia de IA para desempeñar adecuadamente dichas tareas. Dichas obligaciones deben entenderse sin perjuicio de otras obligaciones que tenga el responsable del despliegue en relación con los sistemas de IA de alto riesgo con arreglo al Derecho nacional o de la Unión.

(92) El presente Reglamento se entiende sin perjuicio de la obligación de los empleadores de informar o de informar y consultar a los trabajadores o a sus representantes, en virtud del Derecho o las prácticas nacionales o de la Unión, incluida la Directiva 2002/14/CE del Parlamento Europeo y del Consejo ([39]), sobre la decisión de poner en servicio o utilizar sistemas de IA. Se debe velar por que se informe a los trabajadores y a sus representantes sobre el despliegue previsto de sistemas de IA de alto riesgo en el lugar de trabajo incluso aunque no se cumplan las condiciones de las citadas obligaciones de información o de información y consulta previstas en otros instrumentos jurídicos. Además, este derecho de información es accesorio y necesario para el objetivo de protección de los derechos fundamentales que subyace al presente Reglamento. Por consiguiente, debe establecerse en el presente Reglamento un requisito de información a tal efecto, sin que dicho requisito afecte a ningún derecho vigente de los trabajadores.

(93) Aunque los riesgos relacionados con los sistemas de IA pueden derivarse de su diseño, también pueden derivarse riesgos del uso que se hace de ellos. Por ello, los responsables del despliegue de un sistema de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, como complemento de las obligaciones del proveedor al desarrollar el sistema de IA. Los responsables del despliegue se encuentran en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos que no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los colectivos de personas que probablemente se vean afectados, entre los que se incluyen colectivos vulnerables. Los responsables del despliegue de los sistemas de IA de alto riesgo que se enumeran en un anexo del presente Reglamento también desempeñan un papel fundamental a la hora de informar a las personas físicas y, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, deben, en su caso, informar a las personas físicas de que son objeto de la utilización de un sistema de IA de alto riesgo. Esta información debe incluir la finalidad prevista y el tipo de decisiones que se toman. El responsable del despliegue también debe informar a las personas físicas de su derecho a una explicación con arreglo al presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo que se utilizan a efectos de la garantía del cumplimiento del Derecho, esa obligación debe ejecutarse de conformidad con el artículo 13 de la Directiva (UE) 2016/680.

(94) Todo tratamiento de datos biométricos que se produzca en el marco de la utilización de un sistema de IA para la identificación biométrica con fines de garantía del cumplimiento del Derecho debe cumplir lo dispuesto en el artículo 10 de la Directiva (UE) 2016/680, que permite dicho tratamiento solo cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y cuando así lo autorice el Derecho de la Unión o de los Estados miembros. Dicho uso, cuando esté autorizado, también debe respetar los principios establecidos en el artículo 4, apartado 1, de la Directiva (UE) 2016/680, como, entre otros, que el tratamiento sea lícito y leal, la transparencia, la limitación de la finalidad, la exactitud y la limitación del plazo de conservación.

(95) Sin perjuicio del Derecho de la Unión aplicable, en particular el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, teniendo en cuenta el carácter intrusivo de los sistemas de identificación biométrica remota en diferido, el uso de este tipo de sistemas debe estar sujeto a garantías. Los sistemas de identificación biométrica remota en diferido deben utilizarse siempre de manera proporcionada y legítima, en la medida de lo estrictamente necesario y, por ende, de forma selectiva por lo que respecta a las personas que deben identificarse, la ubicación y el alcance temporal y a partir de un conjunto limitado de datos de grabaciones de vídeo obtenidas legalmente. En cualquier caso, los sistemas de identificación biométrica remota en diferido no deben utilizarse en el marco de la garantía del cumplimiento del Derecho de tal forma que se produzca una vigilancia indiscriminada. Las condiciones para la identificación biométrica remota en diferido en ningún caso deben servir para eludir las condiciones de la prohibición y las estrictas excepciones aplicables a la identificación biométrica remota en tiempo real.

(96) A fin de garantizar eficazmente la protección de los derechos fundamentales, los responsables del despliegue de sistemas de IA de alto riesgo que sean organismos de Derecho público, o las entidades privadas que presten servicios públicos y los responsables del despliegue de determinados sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento, como las entidades bancarias o de seguros, deben llevar a cabo una evaluación de impacto relativa a los derechos fundamentales antes de su puesta en funcionamiento. Algunos servicios importantes para las personas que son de carácter público también pueden ser prestados por entidades privadas. Las entidades privadas que prestan estos servicios públicos se vinculan a funciones de interés público, por ejemplo, en el ámbito de la educación, la asistencia sanitaria, los servicios sociales, la vivienda y la administración de justicia. El objetivo de la evaluación de impacto relativa a los derechos fundamentales es que el responsable del despliegue determine los riesgos específicos para los derechos de las personas o colectivos de personas que probablemente se vean afectados y defina las medidas que deben adoptarse en caso de que se materialicen dichos riesgos. La evaluación de impacto debe

([39]) Directiva 2002/14/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 2002, por la que se establece un marco general relativo a la información y a la consulta de los trabajadores en la Comunidad Europea (DO L 80 de 23.3.2002, p. 29).

llevarse a cabo antes del despliegue del sistema de IA de alto riesgo y debe actualizarse cuando el responsable del despliegue considere que alguno de los factores pertinentes ha cambiado. La evaluación de impacto debe determinar los procesos pertinentes del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista y debe incluir una descripción del plazo de tiempo y la frecuencia en que se pretende utilizar el sistema, así como de las categorías concretas de personas físicas y de colectivos de personas que probablemente se vean afectados por el uso del sistema de IA de alto riesgo en ese contexto de uso específico. La evaluación también debe determinar los riesgos de perjuicio específicos que probablemente afecten a los derechos fundamentales de dichas personas o colectivos. Al llevar a cabo esta evaluación, el responsable del despliegue debe tener en cuenta la información pertinente para una evaluación adecuada del impacto, lo que incluye, por ejemplo, la información facilitada por el proveedor del sistema de IA de alto riesgo en las instrucciones de uso. A la luz de los riesgos detectados, los responsables del despliegue deben determinar las medidas que han de adoptarse en caso de que se materialicen dichos riesgos, entre las que se incluyen, por ejemplo, sistemas de gobernanza para ese contexto de uso específico, como los mecanismos de supervisión humana con arreglo a las instrucciones de uso, los procedimientos de tramitación de reclamaciones y de recurso, ya que podrían ser fundamentales para mitigar los riesgos para los derechos fundamentales en casos de uso concretos. Tras llevar a cabo dicha evaluación de impacto, el responsable del despliegue debe notificarlo a la autoridad de vigilancia del mercado pertinente. Cuando proceda, para recopilar la información pertinente necesaria para llevar a cabo la evaluación de impacto, los responsables del despliegue de un sistema de IA de alto riesgo, en particular cuando el sistema de IA se utilice en el sector público, pueden contar con la participación de las partes interesadas pertinentes, como, por ejemplo, los representantes de colectivos de personas que probablemente se vean afectados por el sistema de IA, expertos independientes u organizaciones de la sociedad civil, en la realización de dichas evaluaciones de impacto y en el diseño de las medidas que deben adoptarse en caso de materialización de los riesgos. La Oficina Europea de Inteligencia Artificial (en lo sucesivo, «Oficina de IA») debe elaborar un modelo de cuestionario con el fin de facilitar el cumplimiento y reducir la carga administrativa para los responsables del despliegue.

(97) El concepto de modelos de IA de uso general debe definirse claramente y diferenciarse del concepto de sistemas de IA con el fin de garantizar la seguridad jurídica. La definición debe basarse en las características funcionales esenciales de un modelo de IA de uso general, en particular la generalidad y la capacidad de realizar de manera competente una amplia variedad de tareas diferenciadas. Estos modelos suelen entrenarse usando grandes volúmenes de datos y a través de diversos métodos, como el aprendizaje autosupervisado, no supervisado o por refuerzo. Los modelos de IA de uso general pueden introducirse en el mercado de diversas maneras, por ejemplo, a través de bibliotecas, interfaces de programación de aplicaciones (API), como descarga directa o como copia física. Estos modelos pueden modificarse o perfeccionarse y transformarse en nuevos modelos. Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen por sí mismos sistemas de IA. Los modelos de IA requieren que se les añadan otros componentes, como, por ejemplo, una interfaz de usuario, para convertirse en sistemas de IA. Los modelos de IA suelen estar integrados en los sistemas de IA y formar parte de dichos sistemas. El presente Reglamento establece normas específicas para los modelos de IA de uso general y para los modelos de IA de uso general que entrañan riesgos sistémicos, que deben aplicarse también cuando estos modelos estén integrados en un sistema de IA o formen parte de un sistema de IA. Debe entenderse que las obligaciones de los proveedores de modelos de IA de uso general deben aplicarse una vez que los modelos de IA de uso general se introduzcan en el mercado. Cuando el proveedor de un modelo de IA de uso general integre un modelo propio en un sistema de IA propio que se comercialice o ponga en servicio, se debe considerar que dicho modelo se ha introducido en el mercado y, por tanto, se deben seguir aplicando las obligaciones establecidas en el presente Reglamento en relación con los modelos, además de las establecidas en relación con los sistemas de IA. En cualquier caso, las obligaciones establecidas en relación con los modelos no deben aplicarse cuando un modelo propio se utilice en procesos puramente internos que no sean esenciales para suministrar un producto o un servicio a un tercero y los derechos de las personas físicas no se vean afectados. Teniendo en cuenta su potencial para causar efectos negativos importantes, los modelos de IA de uso general con riesgo sistémico deben estar siempre sujetos a las obligaciones pertinentes establecidas en el presente Reglamento. La definición no debe incluir los modelos de IA utilizados antes de su introducción en el mercado únicamente para actividades de investigación, desarrollo y creación de prototipos. Lo anterior se entiende sin perjuicio de la obligación de cumplir lo dispuesto en el presente Reglamento cuando, tras haber realizado dichas actividades, el modelo se introduzca en el mercado.

(98) Aunque la generalidad de un modelo también podría determinarse, entre otras cosas, mediante una serie de parámetros, debe considerarse que los modelos que tengan al menos mil millones de parámetros y se hayan entrenado con un gran volumen de datos utilizando la autosupervisión a escala presentan un grado significativo de generalidad y realizan de manera competente una amplia variedad de tareas diferenciadas.

(99) Los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general, ya que permiten la generación flexible de contenidos, por ejemplo, en formato de texto, audio, imágenes o vídeo, que pueden adaptarse fácilmente a una amplia gama de tareas diferenciadas.

(100) Cuando un modelo de IA de uso general esté integrado en un sistema de IA o forme parte de él, este sistema debe considerarse un sistema de IA de uso general cuando, debido a esta integración, el sistema tenga la capacidad de servir a diversos fines. Un sistema de IA de uso general puede utilizarse directamente e integrarse en otros sistemas de IA.

(101) Los proveedores de modelos de IA de uso general tienen una función y una responsabilidad particulares a lo largo de la cadena de valor de la IA, ya que los modelos que suministran pueden constituir la base de diversos sistemas de etapas posteriores, que a menudo son suministrados por proveedores posteriores que necesitan entender bien los modelos y sus capacidades, tanto para permitir la integración de dichos modelos en sus productos como para cumplir sus obligaciones en virtud del presente Reglamento o de otros reglamentos. Por consiguiente, deben establecerse medidas de transparencia proporcionadas, lo que incluye elaborar documentación y mantenerla actualizada y facilitar información sobre el modelo de IA de uso general para su uso por parte de los proveedores posteriores. El proveedor del modelo de IA de uso general debe elaborar y mantener actualizada la documentación técnica con el fin de ponerla a disposición, previa solicitud, de la Oficina de IA y de las autoridades nacionales competentes. Los elementos mínimos que debe contener dicha documentación deben establecerse en anexos específicos del presente Reglamento. La Comisión debe estar facultada para modificar dichos anexos mediante actos delegados en función de los avances tecnológicos.

(102) El *software* y los datos, incluidos los modelos, divulgados con arreglo a una licencia libre y de código abierto que permita compartirlos abiertamente y que los usuarios puedan acceder a ellos, o a versiones modificadas de dicho *software* y dichos datos, o utilizarlos, modificarlos y redistribuirlos libremente, pueden contribuir a la investigación y la innovación en el mercado y pueden ofrecer importantes oportunidades de crecimiento para la economía de la Unión. Debe considerarse que los modelos de IA de uso general divulgados con arreglo a una licencia libre y de código abierto garantizan altos niveles de transparencia y apertura si sus parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se ponen a disposición del público. La licencia debe considerarse libre y de código abierto cuando permita a los usuarios ejecutar, copiar, distribuir, estudiar, modificar y mejorar el *software* y los datos, incluidos los modelos a condición de que se cite al proveedor original del modelo, si se respetan unas condiciones de distribución idénticas o comparables.

(103) Los componentes de IA libres y de código abierto comprenden el *software* y los datos, incluidos los modelos y los modelos de IA de uso general, las herramientas, los servicios y los procesos de un sistema de IA. Los componentes de IA libres y de código abierto pueden suministrarse a través de diferentes canales, lo que incluye la posibilidad de desarrollarlos en repositorios abiertos. A los efectos del presente Reglamento, los componentes de IA que se suministren a cambio de una contraprestación o que se moneticen de cualquier otro modo, como, por ejemplo, mediante la prestación de apoyo técnico u otros servicios en relación con el componente de IA, ya sea a través de una plataforma de *software* o por otros medios, o mediante el uso de datos personales con fines que no se refieran exclusivamente a la mejora de la seguridad, la compatibilidad o la interoperabilidad del *software*, salvo si se trata de operaciones entre microempresas, no deben poder acogerse a las excepciones previstas para los componentes de IA libres y de código abierto. La disponibilidad de un componente de IA a través de repositorios abiertos no debe constituir, de por sí, una monetización.

(104) Los proveedores de modelos de IA de uso general divulgados con arreglo a una licencia libre y de código abierto cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se ponen a disposición del público deben estar sujetos a excepciones por lo que respecta a los requisitos de transparencia que se imponen a los modelos de IA de uso general, a menos que pueda considerarse que presentan un riesgo sistémico, en cuyo caso la circunstancia de que el modelo sea transparente y vaya acompañado de una licencia de código abierto no debe considerarse una razón suficiente para que quede exento del cumplimiento de las obligaciones establecidas en el presente Reglamento. En cualquier caso, dado que la divulgación de modelos de IA de uso general con arreglo a una licencia libre y de código abierto no necesariamente revela información sustancial sobre el conjunto de datos utilizado para entrenar el modelo o realizar ajustes en relación con este ni sobre la manera en que se garantizó el cumplimiento del Derecho en materia de derechos de autor, la excepción prevista para los modelos de IA de uso general en relación con el cumplimiento de los requisitos de transparencia no debe eximir de la obligación de presentar un resumen del contenido utilizado para el entrenamiento del modelo ni de la obligación de adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor, en particular para identificar y respetar la reserva de derechos prevista en el artículo 4, apartado 3, de la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo ([40]).

(105) Los modelos de IA de uso general, en particular los grandes modelos de IA generativos, capaces de generar texto, imágenes y otros contenidos, presentan unas oportunidades de innovación únicas, pero también representan un desafío para los artistas, autores y demás creadores y para la manera en que se crea, distribuye, utiliza y consume su contenido creativo. El desarrollo y el entrenamiento de estos modelos requiere acceder a grandes cantidades de texto, imágenes, vídeos y otros datos. Las técnicas de prospección de textos y datos pueden utilizarse ampliamente en este contexto para la recuperación y el análisis de tales contenidos, que pueden estar protegidos por derechos de autor y derechos afines. Todo uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor. La Directiva (UE) 2019/790 introdujo excepciones y limitaciones que permiten reproducciones y extracciones de obras y otras prestaciones con fines de prospección de textos y datos en determinadas circunstancias. Con arreglo

([40]) Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (DO L 130 de 17.5.2019, p. 92).

a estas normas, los titulares de derechos pueden optar por reservarse sus derechos en relación con sus obras u otras prestaciones para evitar la prospección de textos y datos, salvo que su finalidad sea la investigación científica. Cuando el titular del derecho se haya reservado de manera adecuada el derecho de exclusión, los proveedores de modelos de IA de uso general deben obtener su autorización para llevar a cabo una prospección de textos y datos con dichas obras.

(106) Los proveedores que introduzcan modelos de IA de uso general en el mercado de la Unión deben garantizar el cumplimiento de las obligaciones pertinentes establecidas en el presente Reglamento. A tal fin, los proveedores de modelos de IA de uso general deben adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para detectar y cumplir la reserva de derechos expresada por los titulares de derechos con arreglo al artículo 4, apartado 3, de la Directiva (UE) 2019/790. Todo proveedor que introduzca un modelo de IA de uso general en el mercado de la Unión debe cumplir esta obligación, independientemente de la jurisdicción en la que tengan lugar los actos pertinentes en materia de derechos de autor que sustentan el entrenamiento de dichos modelos de IA de uso general. Esta medida es necesaria para garantizar unas condiciones de competencia equitativas entre los proveedores de modelos de IA de uso general que impidan que un proveedor obtenga una ventaja competitiva en el mercado de la Unión aplicando normas en materia de derechos de autor menos estrictas que las establecidas en la Unión.

(107) Con el fin de aumentar la transparencia en relación con los datos utilizados en el entrenamiento previo y el entrenamiento de los modelos de IA de uso general, incluidos los textos y los datos protegidos por el Derecho en materia de derechos de autor, procede que los proveedores de dichos modelos elaboren y pongan a disposición del público un resumen suficientemente detallado de los contenidos utilizados para el entrenamiento del modelo de IA de uso general. Este resumen debe tener debidamente en cuenta la necesidad de proteger los secretos comerciales y la información empresarial confidencial y, al mismo tiempo, debe ser exhaustivo en general en su alcance en vez de técnicamente detallado, a fin de facilitar que las partes con intereses legítimos, incluidos los titulares de derechos de autor, ejerzan y hagan cumplir sus derechos en virtud del Derecho de la Unión, por ejemplo, enumerando los principales conjuntos o recopilaciones de datos que hayan servido para entrenar al modelo, como los grandes archivos de datos o bases de datos privados o públicos, y proporcionando una explicación descriptiva sobre otras fuentes de datos utilizadas. Conviene que la Oficina de IA proporcione un modelo para el resumen, que debe ser sencillo y eficaz y permitir que el proveedor proporcione el resumen requerido en forma descriptiva.

(108) Por lo que se refiere a las obligaciones impuestas a los proveedores de modelos de IA de uso general de adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y de poner a disposición del público un resumen de los contenidos utilizados para el entrenamiento, la Oficina de IA debe supervisar si el proveedor ha cumplido dichas obligaciones sin verificar ni proceder a una evaluación obra por obra de los datos de entrenamiento en cuanto al respeto de los derechos de autor. El presente Reglamento no afecta al cumplimiento de las normas en materia de derechos de autor previstas en el Derecho de la Unión.

(109) El cumplimiento de las obligaciones aplicables a los proveedores de modelos de IA de uso general debe ser proporcionado y adecuado al tipo de proveedor de modelos. Debe eximirse de la obligación de cumplimiento a las personas que desarrollan o utilizan modelos con fines no profesionales o de investigación científica. No obstante, debe animarse a estas personas a cumplir voluntariamente estos requisitos. Sin perjuicio del Derecho de la Unión en materia de derechos de autor, el cumplimiento de esas obligaciones debe tener debidamente en cuenta el tamaño del proveedor y permitir formas simplificadas de cumplimiento para las pymes, incluidas las empresas emergentes, que no deben suponer un coste excesivo ni desincentivar el uso de dichos modelos. En caso de que se modifique o ajuste un modelo, las obligaciones de los proveedores de modelos de IA de uso general deben limitarse a esa modificación o esos ajustes, por ejemplo, complementando la documentación técnica ya existente con información sobre las modificaciones, incluidas las nuevas fuentes de datos de entrenamiento, para cumplir las obligaciones relacionadas con la cadena de valor establecidas en el presente Reglamento.

(110) Los modelos de IA de uso general pueden plantear riesgos sistémicos, por ejemplo, cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, perturbaciones de sectores críticos y consecuencias graves para la salud y la seguridad públicas, cualquier efecto negativo real o razonablemente previsible sobre los procesos democráticos y la seguridad pública y económica o la difusión de contenidos ilícitos, falsos o discriminatorios. Debe entenderse que los riesgos sistémicos aumentan con las capacidades y el alcance de los modelos, pueden surgir durante todo el ciclo de vida del modelo y se ven influidos por las condiciones de uso indebido, la fiabilidad del modelo, la equidad y la seguridad del modelo, el nivel de autonomía del modelo, su acceso a herramientas, modalidades novedosas o combinadas, las estrategias de divulgación y distribución, la posibilidad de eliminar las salvaguardias y otros factores. En particular, los enfoques internacionales han establecido hasta la fecha la necesidad de prestar atención a los riesgos derivados de posibles usos indebidos intencionados o de problemas en materia de control relacionados con la armonización con la intención humana no deseados, a los riesgos químicos, biológicos, radiológicos y nucleares, como las maneras en que las barreras a la entrada pueden reducirse, también

para el desarrollo, el diseño, la adquisición o el uso de armas, a las cibercapacidades ofensivas, como las maneras en que pueden propiciarse el descubrimiento, la explotación o el uso operativo de vulnerabilidades, a los efectos de la interacción y el uso de herramientas, incluida, por ejemplo, la capacidad de controlar sistemas físicos e interferir en el funcionamiento de infraestructuras críticas, a los riesgos derivados del hecho que los modelos hagan copias de sí mismos o se «autorrepliquen» o entrenen a otros modelos, a las maneras en que los modelos pueden dar lugar a sesgos dañinos y discriminación que entrañan riesgos para las personas, las comunidades o las sociedades, a la facilitación de la desinformación o el menoscabo de la intimidad, que suponen una amenaza para los valores democráticos y los derechos humanos, al riesgo de que un acontecimiento concreto dé lugar a una reacción en cadena con efectos negativos considerables que podrían afectar incluso a una ciudad entera, un ámbito de actividad entero o una comunidad entera.

(111) Conviene establecer una metodología para la clasificación de los modelos de IA de uso general como modelos de IA de uso general con riesgos sistémicos. Dado que los riesgos sistémicos se derivan de capacidades especialmente elevadas, debe considerarse que un modelo de IA de uso general presenta riesgos sistémicos si tiene capacidades de gran impacto —evaluadas mediante herramientas y metodologías técnicas adecuadas— o unas repercusiones considerables en el mercado interior debido a su alcance. Las capacidades de gran impacto en modelos de IA de uso general son capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados. La introducción en el mercado de un modelo o las interacciones de los responsables del despliegue con él permiten comprender mejor el conjunto de sus capacidades. Según el estado de la técnica en el momento de la entrada en vigor del presente Reglamento, la cantidad acumulada de cálculo utilizado para el entrenamiento del modelo de IA de uso general, medida en operaciones de coma flotante, es una de las aproximaciones pertinentes para las capacidades del modelo. La cantidad acumulada de cálculo utilizado para el entrenamiento incluye los cálculos utilizados en las distintas actividades y métodos destinados a mejorar las capacidades del modelo antes del despliegue, como el entrenamiento previo, la generación de datos sintéticos y la realización de ajustes. Por lo tanto, debe establecerse un umbral inicial de operaciones de coma flotante que, de ser alcanzado por un modelo de IA de uso general, dé lugar a la presunción de que el modelo es un modelo de IA de uso general con riesgos sistémicos. Este umbral deberá irse ajustando para reflejar los cambios tecnológicos e industriales, como las mejoras algorítmicas o el aumento de la eficiencia del hardware, y debe complementarse con parámetros de referencia e indicadores de la capacidad de los modelos. Para fundamentar esto, la Oficina de IA debe colaborar con la comunidad científica, la industria, la sociedad civil y otros expertos. Los umbrales, así como las herramientas y los parámetros de referencia para la evaluación de las capacidades de gran impacto, deben servir para predecir con fiabilidad la generalidad, las capacidades y el riesgo sistémico asociado de los modelos de IA de uso general, y podrían tener en cuenta la manera en que el modelo se introducirá en el mercado o el número de usuarios a los que podría afectar. Para complementar este sistema, la Comisión debe poder adoptar decisiones individuales por las que se designe un modelo de IA de uso general como modelo de IA de uso general con riesgo sistémico si se determina que dicho modelo tiene capacidades o repercusiones equivalentes a las reflejadas por el umbral establecido. Dicha decisión debe adoptarse atendiendo a una evaluación global de los criterios para la designación de modelos de IA de uso general con riesgo sistémico establecidos en un anexo del presente Reglamento, como la calidad o el tamaño del conjunto de datos de entrenamiento, el número de usuarios profesionales y finales, sus modalidades de entrada y de salida, su nivel de autonomía y escalabilidad o las herramientas a las que tiene acceso. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de uso general con riesgo sistémico, la Comisión debe tener en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de uso general presenta riesgos sistémicos.

(112) También es necesario aclarar un procedimiento para la clasificación de un modelo de IA de uso general con riesgos sistémicos. Debe presumirse que un modelo de IA de uso general que alcanza el umbral aplicable para las capacidades de gran impacto es un modelo de IA de uso general con riesgo sistémico. El proveedor debe enviar una notificación a la Oficina de IA a más tardar dos semanas después de que se cumplan los requisitos o de que se sepa que un modelo de IA de uso general cumplirá los requisitos que conducen a la presunción. Esto es especialmente pertinente en relación con el umbral de operaciones de coma flotante, ya que el entrenamiento de los modelos de IA de uso general requiere una planificación considerable que incluye la asignación previa de recursos computacionales y, por tanto, los proveedores de modelos de IA de uso general pueden saber si su modelo alcanzará el umbral antes del fin del entrenamiento. En el contexto de dicha notificación, el proveedor debe poder demostrar que, debido a sus características específicas, un modelo de IA de uso general no presenta excepcionalmente riesgos sistémicos y que, por tanto, no debe clasificarse como modelo de IA de uso general con riesgos sistémicos. Esa información es valiosa para que la Oficina de IA anticipe la introducción en el mercado de modelos de IA de uso general con riesgos sistémicos y para que los proveedores pueden empezar a colaborar con la Oficina de IA en una fase temprana. Dicha información es especialmente importante cuando esté previsto divulgar un modelo de IA de uso general como

modelo de código abierto, dado que, tras la divulgación de modelos de código abierto, puede resultar más difícil aplicar las medidas necesarias para garantizar el cumplimiento de las obligaciones establecidas en el presente Reglamento.

(113) Si la Comisión descubre que un modelo de IA de uso general del que no tenía conocimiento o que el proveedor pertinente no le había notificado cumple los requisitos para ser clasificado como modelo de IA de uso general con riesgo sistémico, la Comisión debe estar facultada para designarlo. Además de las actividades de supervisión de la Oficina de IA, un sistema de alertas cualificadas debe garantizar que la Oficina de IA sea informada por el grupo de expertos científicos de la existencia de modelos de IA de uso general que podrían ser clasificados como modelos de IA de uso general con riesgo sistémico.

(114) Los proveedores de modelos de IA de uso general que presenten riesgos sistémicos deben estar sujetos, además de a las obligaciones impuestas a los proveedores de modelos de IA de uso general, a obligaciones encaminadas a detectar y atenuar dichos riesgos y a garantizar un nivel adecuado de protección en materia de ciberseguridad, independientemente de si dichos modelos se ofrecen como modelos independientes o están integrados en sistemas de IA o en productos. Para alcanzar esos objetivos, el presente Reglamento debe exigir a los proveedores que lleven a cabo las evaluaciones de los modelos necesarias, en particular antes de la primera introducción en el mercado, y que, por ejemplo, lleven a cabo y documenten pruebas de simulación de adversarios, también, según proceda, mediante pruebas externas independientes o pruebas internas. Además, los proveedores de modelos de IA de uso general con riesgos sistémicos deben evaluar y mitigar continuamente los riesgos sistémicos, por ejemplo, mediante el establecimiento de políticas de gestión de riesgos, como procesos de rendición de cuentas y gobernanza, la puesta en práctica de la vigilancia poscomercialización, la adopción de medidas adecuadas durante todo el ciclo de vida del modelo y la cooperación con los agentes pertinentes a lo largo de la cadena de valor de la IA.

(115) Los proveedores de modelos de IA de uso general con riesgos sistémicos deben evaluar y mitigar los posibles riesgos sistémicos. Si, a pesar de los esfuerzos por detectar y prevenir los riesgos relacionados con un modelo de IA de uso general que pueda presentar riesgos sistémicos, el desarrollo o el uso del modelo provoca un incidente grave, el proveedor del modelo de IA de uso general debe, sin demora indebida, hacer un seguimiento del incidente y comunicar toda la información pertinente y las posibles medidas correctoras a la Comisión y a las autoridades nacionales competentes. Además, los proveedores deben garantizar que el modelo y su infraestructura física, si procede, tengan un nivel adecuado de protección en materia de ciberseguridad durante todo el ciclo de vida del modelo. La protección en materia de ciberseguridad relacionada con los riesgos sistémicos asociados al uso malintencionado o a los ataques debe tener debidamente en cuenta las fugas accidentales de modelos, las divulgaciones no autorizadas, la elusión de las medidas de seguridad y la defensa contra los ciberataques, el acceso no autorizado o el robo de modelos. Esa protección podría facilitarse asegurando los pesos, los algoritmos, los servidores y los conjuntos de datos del modelo, por ejemplo, mediante medidas de seguridad operativa para la seguridad de la información, medidas específicas en materia de ciberseguridad, soluciones técnicas adecuadas y establecidas y controles de acceso cibernéticos y físicos, en función de las circunstancias pertinentes y los riesgos existentes.

(116) La Oficina de IA debe fomentar y facilitar la elaboración, revisión y adaptación de códigos de buenas prácticas, teniendo en cuenta los enfoques internacionales. Podría invitarse a participar a todos los proveedores de modelos de IA de uso general. Para garantizar que los códigos de buenas prácticas reflejen el estado actual de la técnica y tengan debidamente en cuenta perspectivas distintas, la Oficina de IA debe colaborar con las autoridades nacionales competentes pertinentes y, cuando proceda, podrá consultar a organizaciones de la sociedad civil y a otras partes interesadas y expertos pertinentes, incluido el Grupo de Expertos Científicos, por lo que respecta a la elaboración de dichos códigos. Los códigos de buenas prácticas deben comprender las obligaciones de los proveedores de modelos de IA de uso general y de modelos de IA de uso general que presenten riesgos sistémicos. Además, en lo que respecta a los riesgos sistémicos, los códigos de buenas prácticas deben ayudar a establecer una taxonomía de riesgos en la que figuren el tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluidas sus fuentes. Asimismo, los códigos de buenas prácticas deben centrarse en medidas específicas de evaluación y reducción de riesgos.

(117) Los códigos de buenas prácticas deben constituir una herramienta fundamental para el cumplimiento adecuado de las obligaciones previstas en el presente Reglamento para los proveedores de modelos de IA de uso general. Los proveedores deben poder basarse en códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. Mediante actos de ejecución, la Comisión podrá decidir aprobar un código de buenas prácticas y conferirle una validez general dentro de la Unión o, alternativamente, establecer normas comunes para la puesta en práctica de las obligaciones pertinentes si, para el momento en que el presente Reglamento sea aplicable, no ha podido finalizarse un código de buenas prácticas o la Oficina de IA no lo considera adecuado. Una vez que se haya

publicado una norma armonizada y que la Oficina de IA la considere adecuada para cubrir las obligaciones pertinentes, el cumplimiento de una norma armonizada europea debe dar a los proveedores la presunción de conformidad. Además, los proveedores de modelos de IA de uso general deben poder demostrar el cumplimiento utilizando medios alternativos adecuados si no se dispone de códigos de buenas prácticas o de normas armonizadas, o si deciden no basarse en ellos.

(118) El presente Reglamento regula los sistemas de IA y modelos de IA imponiendo determinados requisitos y obligaciones a los agentes pertinentes del mercado que los introduzcan en el mercado, los pongan en servicio o los utilicen en la Unión, complementando así las obligaciones de los prestadores de servicios intermediarios que integren dichos sistemas o modelos en sus servicios, regulados por el Reglamento (UE) 2022/2065. En la medida en que dichos sistemas o modelos estén integrados en plataformas en línea de muy gran tamaño o en motores de búsqueda en línea de muy gran tamaño que hayan sido designados, están sujetos al marco de gestión de riesgos establecido en el Reglamento (UE) 2022/2065. Por consiguiente, debe presumirse que se han cumplido las obligaciones correspondientes del presente Reglamento a menos que surjan riesgos sistémicos significativos no cubiertos por el Reglamento (UE) 2022/2065 y se detecten en dichos modelos. En este marco, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño están obligados a evaluar los posibles riesgos sistémicos derivados del diseño, el funcionamiento y el uso de sus servicios, incluido el modo en que el diseño de los sistemas algorítmicos utilizados en el servicio puede contribuir a dichos riesgos, así como los riesgos sistémicos derivados de posibles usos indebidos. Dichos prestadores también están obligados a adoptar las medidas de reducción de riesgos adecuadas respetando los derechos fundamentales.

(119) Tomando en consideración el rápido ritmo de innovación y la evolución tecnológica de los servicios digitales incluidos en el ámbito de aplicación de diferentes instrumentos del Derecho de la Unión, en particular teniendo en cuenta el uso y la percepción de sus destinatarios, los sistemas de IA sujetos al presente Reglamento pueden prestarse como servicios intermediarios, o partes de estos, en el sentido del Reglamento (UE) 2022/2065, que debe interpretarse de manera tecnológicamente neutra. Por ejemplo, los sistemas de IA pueden utilizarse para ofrecer motores de búsqueda en línea, en particular en la medida en que un sistema de IA, como un chatbot en línea, efectúe búsquedas, en principio, en todos los sitios web, incorpore a continuación los resultados a sus conocimientos existentes y utilice los conocimientos actualizados para generar una única información de salida que combine diferentes fuentes de información.

(120) Además, las obligaciones impuestas a los proveedores y a los responsables del despliegue de determinados sistemas de IA en el presente Reglamento destinadas a permitir que se detecte y divulgue que los resultados de salida de dichos sistemas han sido generados o manipulados de manera artificial resultan especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular a las obligaciones de los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño de detectar y mitigar los riesgos sistémicos que pueden surgir de la divulgación de contenidos que hayan sido generados o manipulados de manera artificial, en particular el riesgo de los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, también a través de la desinformación.

(121) La normalización debe desempeñar un papel fundamental para proporcionar soluciones técnicas a los proveedores para garantizar el cumplimiento del presente Reglamento, en consonancia con el estado actual de la técnica, para promover la innovación, así como la competitividad y el crecimiento en el mercado único. El cumplimiento de las normas armonizadas definidas en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([41]), que generalmente se espera que reflejen el estado actual de la técnica, debe ser un medio para que los proveedores demuestren la conformidad con los requisitos previstos en el presente Reglamento. Por consiguiente, debe fomentarse una representación equilibrada de los intereses de todas las partes interesadas pertinentes —en particular las pymes, las organizaciones de consumidores y las partes interesadas de los ámbitos social y medioambiental— en la elaboración de normas, de conformidad con los artículos 5 y 6 del Reglamento (UE) n.º 1025/2012. A fin de facilitar el cumplimiento, la Comisión debe emitir las peticiones de normalización sin demora indebida. Al preparar la petición de normalización, la Comisión debe consultar al foro consultivo y al Consejo de IA para recabar los conocimientos especializados pertinentes. No obstante, a falta de referencias pertinentes a las normas armonizadas, la Comisión debe poder establecer, mediante actos de ejecución y previa consulta al foro consultivo, especificaciones comunes para determinados requisitos previstos en el presente Reglamento. Las especificaciones comunes deben ser una solución alternativa excepcional para facilitar la obligación del proveedor de cumplir los requisitos del presente Reglamento cuando ninguna de las organizaciones europeas de normalización haya aceptado la petición de normalización, cuando las normas armonizadas pertinentes respondan de forma insuficiente a las preocupaciones en materia de derechos fundamentales, cuando las normas armonizadas no cumplan la petición o cuando se produzcan retrasos en la adopción de una norma armonizada adecuada. Cuando dichos retrasos en la adopción de una norma armonizada se deban a la complejidad técnica de dicha norma, la

([41]) 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).

Comisión debe tenerlo en cuenta antes de considerar la posibilidad de establecer especificaciones comunes. Se anima a la Comisión a que, a la hora de elaborar especificaciones comunes, coopere con los socios internacionales y los organismos internacionales de normalización.

(122) Conviene que, sin perjuicio del uso de normas armonizadas y especificaciones comunes, se presuma que los proveedores de un sistema de IA de alto riesgo que haya sido entrenado y probado con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto que se utilice el sistema de IA cumplen la medida pertinente prevista en el requisito en materia de gobernanza de datos establecido en el presente Reglamento. Sin perjuicio de los requisitos relacionados con la solidez y la precisión establecidos en el presente Reglamento, de conformidad con el artículo 54, apartado 3, del Reglamento (UE) 2019/881, debe presumirse que los sistemas de IA de alto riesgo que cuenten con una certificación o una declaración de conformidad en virtud de un esquema de certificación de la ciberseguridad con arreglo a dicho Reglamento y cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* cumplen el requisito de ciberseguridad del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad, o partes de estos, contemplen dicho requisito. Esto se entiende sin perjuicio del carácter voluntario de dicho esquema de ciberseguridad.

(123) A fin de garantizar que los sistemas de IA de alto riesgo sean altamente fiables, debe someterse a dichos sistemas a una evaluación de la conformidad antes de su introducción en el mercado o puesta en servicio.

(124) Para reducir al mínimo la carga que deben soportar los operadores y evitar posibles duplicidades, conviene, en el caso de los sistemas de IA de alto riesgo asociados a productos regulados por la legislación de armonización de la Unión vigente basada en el nuevo marco legislativo, que la conformidad de dichos sistemas de IA con los requisitos establecidos en el presente Reglamento se evalúe en el marco de la evaluación de la conformidad ya prevista en dicha legislación. Por lo tanto, la aplicabilidad de los requisitos del presente Reglamento no debe afectar a la lógica, la metodología o la estructura general específicas de la evaluación de la conformidad prevista en los actos legislativos de armonización pertinentes de la Unión.

(125) Dada la complejidad de los sistemas de IA de alto riesgo y los riesgos asociados a ellos, es importante desarrollar un procedimiento adecuado de evaluación de la conformidad de los sistemas de IA de alto riesgo en el que participen organismos notificados, denominado «evaluación de la conformidad de terceros». No obstante, habida cuenta de la experiencia actual de los profesionales que realizan la certificación previa a la comercialización en el campo de la seguridad de los productos y de la distinta naturaleza de los riesgos implicados, procede limitar, al menos en la fase inicial de aplicación del presente Reglamento, el alcance de las evaluaciones externas de la conformidad 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 biometría.

(126) Para poder realizar las evaluaciones de la conformidad de terceros cuando así se les exija, las autoridades nacionales competentes deben notificar, en virtud del presente Reglamento, a los organismos notificados, siempre que cumplan una serie de requisitos, en particular en lo que respecta a su independencia, sus competencias y la ausencia de conflictos de intereses, así como requisitos adecuados de ciberseguridad. Las autoridades nacionales competentes deben enviar la notificación de dichos organismos a la Comisión y a los demás Estados miembros a través del sistema de notificación electrónica desarrollado y gestionado por la Comisión con arreglo a lo dispuesto en el artículo R23 del anexo I de la Decisión n.º 768/2008/CE.

(127) En consonancia con los compromisos contraídos por la Unión en virtud del Acuerdo sobre Obstáculos Técnicos al Comercio, de la Organización Mundial del Comercio, es adecuado facilitar el reconocimiento mutuo de los resultados de las evaluaciones de la conformidad realizadas por organismos de evaluación de la conformidad competentes, con independencia del territorio en el que estén establecidos, siempre que dichos organismos de evaluación de la conformidad establecidos con arreglo al Derecho de un tercer país cumplan los requisitos aplicables del presente Reglamento y la Unión haya celebrado un acuerdo en ese sentido. En este contexto, la Comisión debe estudiar activamente posibles instrumentos internacionales a tal efecto y, en particular, procurar celebrar acuerdos de reconocimiento mutuo con terceros países.

(128) En consonancia con el concepto comúnmente establecido de «modificación sustancial» de los productos regulados por los actos legislativos de armonización de la Unión, conviene que, cada vez que se produzca un cambio que pueda afectar al cumplimiento del presente Reglamento por parte de un sistema de IA de alto riesgo (por ejemplo, un cambio de sistema operativo o de arquitectura de *software*) o cuando cambie la finalidad prevista del sistema, dicho sistema de IA se considere un sistema de IA nuevo que debe someterse a una nueva evaluación de la conformidad. Sin embargo, los cambios que se produzcan en el algoritmo y en el funcionamiento de los sistemas de IA que sigan «aprendiendo» después de su introducción en el mercado o su puesta en servicio, a saber, adaptando automáticamente el modo en que desempeñan sus funciones, no deben constituir una modificación sustancial, siempre que dichos cambios hayan sido predeterminados por el proveedor y se hayan evaluado en el momento de la evaluación de la conformidad.

(129) 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 interior. En el caso de los sistemas de IA de alto riesgo integrados en un producto, se debe colocar un marcado CE físico, que puede complementarse con un marcado CE digital. En el caso de los sistemas de IA de alto riesgo que solo se proporcionen digitalmente, debe utilizarse un marcado CE digital. 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.

(130) En determinadas condiciones, la rápida disponibilidad de tecnologías innovadoras puede ser crucial para la salud y la seguridad de las personas, la protección del medio ambiente y la mitigación del cambio climático, y para la sociedad en su conjunto. Por consiguiente, resulta oportuno que las autoridades de vigilancia del mercado puedan autorizar, por motivos excepcionales de seguridad pública o con vistas a proteger la vida y la salud de personas físicas, el medio ambiente y activos fundamentales de la industria y de las infraestructuras, 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. En situaciones debidamente justificadas previstas en el presente Reglamento, las autoridades garantes del cumplimiento del Derecho o las autoridades de protección civil podrán poner en servicio un sistema de IA de alto riesgo específico sin la autorización de la autoridad de vigilancia del mercado, siempre que se solicite la autorización durante el uso o después de este sin demora indebida.

(131) Con el objetivo de facilitar la labor de la Comisión y de los Estados miembros en el ámbito de la IA, así como de incrementar la transparencia de cara al público, debe exigirse a los proveedores de sistemas de IA de alto riesgo que no estén asociados a productos que entren dentro del ámbito de aplicación de los actos legislativos de armonización de la Unión que sean pertinentes y estén en vigor, y a los proveedores que consideren que alguno de los sistemas de IA enumerados en los casos de uso de alto riesgo en un anexo del presente Reglamento no es de alto riesgo sobre la base de una excepción que se registren y que registren información sobre sus sistemas de IA en una base de datos de la UE, de cuya creación y gestión se encargará la Comisión. Antes de utilizar tal sistema de IA enumerado en los casos de uso de alto riesgo en un anexo del presente Reglamento, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades, órganos u organismos públicos deben registrarse en dicha base de datos y seleccionar el sistema que tengan previsto utilizar. Los demás responsables del despliegue deben poder efectuar dicho registro con carácter voluntario. Esta sección de la base de datos de la UE debe ser de acceso público y gratuito, debe ser fácil navegar por la información, y esta ha de ser comprensible y legible por máquina. La base de datos de la UE también debe ser fácil de utilizar, por ejemplo, proporcionando funcionalidades de búsqueda, también a través de palabras clave, que permitan al público en general encontrar la información que debe presentarse para el registro de los sistemas de IA de alto riesgo y relativa a los casos de uso de sistemas de IA de alto riesgo contemplados en un anexo del presente Reglamento, a la que corresponden los sistemas de IA de alto riesgo. También debe registrarse en la base de datos de la UE toda modificación sustancial de sistemas de IA de alto riesgo. En el caso de los sistemas de IA de alto riesgo en el ámbito de la garantía del cumplimiento del Derecho y de la gestión de la migración, el asilo y el control fronterizo, las obligaciones de registro deben cumplirse en una sección segura no pública de la base de datos de la UE. El acceso a esa sección debe limitarse estrictamente a la Comisión y a las autoridades de vigilancia del mercado en lo que respecta a su sección nacional de dicha base de datos. Los sistemas de IA de alto riesgo en el ámbito de las infraestructuras críticas solo deben registrarse a nivel nacional. La Comisión debe ser la responsable del tratamiento de la base de datos de la UE, de conformidad con el Reglamento (UE) 2018/1725. Con vistas a garantizar la funcionalidad plena de la base de datos de la UE una vez que esté en funcionamiento, el procedimiento para su creación debe comprender el desarrollo de especificaciones funcionales por parte de la Comisión y la redacción de un informe de auditoría independiente. Al ejercer sus funciones como responsable del tratamiento de la base de datos de la UE, la Comisión debe tener en cuenta los riesgos de ciberseguridad. Con el fin de maximizar la disponibilidad y el uso de la base de datos de la UE por parte del público, la base de datos de la UE y la información facilitada a través de ella deben cumplir los requisitos establecidos en la Directiva (UE) 2019/882.

(132) Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden plantear riesgos específicos de suplantación o engaño, con independencia de si cumplen las condiciones para ser considerados 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 y a excepciones específicas a fin de tener en cuenta las necesidades especiales de la garantía del cumplimiento del Derecho. En particular, es preciso comunicar a las personas físicas que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física normalmente informada y razonablemente atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Al aplicar dicha obligación, deben tenerse en cuenta las características de las personas físicas pertenecientes a colectivos vulnerables debido a su edad o discapacidad en la medida en que el sistema de IA esté destinado a interactuar también con dichos colectivos. Además, es preciso notificar a las personas físicas cuando estén expuestas a sistemas de IA que, mediante el tratamiento de sus datos biométricos, puedan determinar o inferir sus emociones o intenciones o incluirlas en categorías específicas. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de ojos, los tatuajes, los rasgos personales, el origen étnico o las preferencias e intereses personales. Esta información y estas notificaciones deben facilitarse en formatos accesibles a las personas con discapacidad.

(133) Una diversidad de sistemas de IA puede generar grandes cantidades de contenidos sintéticos que para las personas cada vez es más difícil distinguir del contenido auténtico generado por seres humanos. La amplia disponibilidad y las crecientes capacidades de dichos sistemas tienen importantes repercusiones en la integridad del ecosistema de la información y en la confianza en este, haciendo surgir nuevos riesgos de desinformación y manipulación a escala, fraude, suplantación de identidad y engaño a los consumidores. En vista de estos efectos, el rápido desarrollo tecnológico y la necesidad de nuevos métodos y técnicas para asegurar la trazabilidad del origen de la información, procede exigir a los proveedores de tales sistemas que integren soluciones técnicas que permitan marcar, en un formato legible por máquina, y detectar que el resultado de salida ha sido generado o manipulado por un sistema de IA y no por un ser humano. Dichas técnicas y métodos deben ser lo suficientemente fiables, interoperables, eficaces y sólidos, en la medida en que sea técnicamente viable, teniendo en cuenta las técnicas disponibles o una combinación de dichas técnicas, como marcas de agua, identificación de metadatos, métodos criptográficos para demostrar la procedencia y la autenticidad del contenido, métodos de registro, impresiones dactilares u otras técnicas, según proceda. A la hora de aplicar esta obligación, los proveedores también deben tener en cuenta las especificidades y las limitaciones de los diferentes tipos de contenidos y los avances tecnológicos y del mercado pertinentes en ese ámbito, tal como se refleja en el estado de la técnica generalmente reconocido. Dichas técnicas y métodos pueden implantarse a nivel de sistema de IA o a nivel de modelo de IA, incluidos modelos de IA de uso general que generan contenidos, facilitando así el cumplimiento de esta obligación por parte del proveedor posterior del sistema de IA. Para garantizar la proporcionalidad, conviene prever que esta obligación de marcado no se aplique a los sistemas de IA que desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica.

(134) Además de las soluciones técnicas utilizadas por los proveedores del sistema de IA, los responsables del despliegue que utilicen un sistema de IA para generar o manipular un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeje notablemente a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos (ultrasuplantaciones) deben también hacer público, de manera clara y distinguible, que este contenido ha sido creado o manipulado de manera artificial etiquetando los resultados de salida generados por la IA en consecuencia e indicando su origen artificial. El cumplimiento de esta obligación de transparencia no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida obstaculiza el derecho a la libertad de expresión y el derecho a la libertad de las artes y de las ciencias, garantizados por la Carta, en particular cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, con sujeción a unas garantías adecuadas para los derechos y libertades de terceros. En tales casos, la obligación de transparencia en relación con las ultrasuplantaciones establecida en el presente Reglamento se limita a revelar la existencia de tales contenidos generados o manipulados de una manera adecuada que no obstaculice la presentación y el disfrute de la obra, también su explotación y uso normales, al tiempo que se conservan la utilidad y la calidad de la obra. Además, también conviene prever una obligación de divulgación similar en relación con el texto generado o manipulado por una IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado por la IA haya sido sometido a un proceso de revisión humana o de control editorial y que una persona física o jurídica ejerza la responsabilidad editorial de la publicación del contenido.

(135) Sin perjuicio del carácter obligatorio y de la plena aplicabilidad de las obligaciones de transparencia, la Comisión podrá también fomentar y facilitar la elaboración de códigos de buenas prácticas a escala de la Unión, a fin de facilitar la aplicación eficaz de las obligaciones en materia de detección y etiquetado de contenidos generados o manipulados de manera artificial, también para apoyar disposiciones prácticas para que, según proceda, los mecanismos de detección sean accesibles y facilitar la cooperación con otros agentes de la cadena de valor, difundiendo los contenidos o comprobando su autenticidad y procedencia, a fin de que el público pueda distinguir efectivamente los contenidos generados por IA.

(136) Las obligaciones impuestas a los proveedores y a los responsables del despliegue de determinados sistemas de IA en el presente Reglamento destinadas a permitir que se detecte y divulgue que los resultados de salida de dichos sistemas han sido generados o manipulados de manera artificial resultan especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular en lo referente a las obligaciones de los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño para detectar y mitigar los riesgos sistémicos que pueden surgir de la divulgación de contenidos que hayan sido generados o manipulados de manera artificial, en particular el riesgo de los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, como a través de la desinformación. La exigencia de etiquetar los contenidos generados por sistemas de IA con arreglo al presente Reglamento se entiende sin perjuicio de la obligación prevista en el artículo 16, apartado 6, del Reglamento (UE) 2022/2065 para los prestadores de servicios de alojamiento de datos de tratar las notificaciones que reciban sobre contenidos ilícitos en virtud del artículo 16, apartado 1, de dicho Reglamento, y no debe influir en la evaluación y la decisión sobre el carácter ilícito del contenido de que se trate. Dicha evaluación debe realizarse únicamente con referencia a las normas que rigen la legalidad del contenido.

(137) El cumplimiento de las obligaciones de transparencia aplicables a los sistemas de IA que entran en el ámbito de aplicación del presente Reglamento no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida es lícito en virtud del presente Reglamento o de otras disposiciones del Derecho de la Unión y de los Estados miembros, y debe entenderse sin perjuicio de otras obligaciones de transparencia aplicables a los responsables del despliegue de sistemas de IA establecidas en el Derecho de la Unión o nacional.

(138) La IA es una familia de tecnologías de rápida evolución que requiere vigilancia regulatoria y un espacio seguro y controlado para la experimentación, así como que se garantice la innovación responsable y la integración de salvaguardias éticas y medidas de reducción de riesgos adecuadas. Para conseguir un marco jurídico que promueva la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones, los Estados miembros deben velar por que sus autoridades nacionales competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional que facilite 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. Los Estados miembros también podrían cumplir esta obligación participando en los espacios controlados de pruebas ya existentes o estableciendo un espacio de pruebas conjuntamente con las autoridades competentes de uno o varios Estados miembros, en la medida en que dicha participación proporcione un nivel de cobertura nacional equivalente para los Estados miembros participantes. Los espacios controlados de pruebas para la IA podrían establecerse de forma física, digital o híbrida y podrán albergar productos tanto físicos como digitales. Las autoridades que los creen deben también garantizar que los espacios controlados de pruebas para la IA dispongan de recursos adecuados para su funcionamiento, incluidos recursos financieros y humanos.

(139) Los espacios controlados de pruebas para la IA 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 otras disposiciones pertinentes del Derecho de la Unión y nacional. Además, los espacios controlados de pruebas para la IA deben tener por objeto mejorar 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, de facilitar el aprendizaje normativo de las autoridades y empresas, también con vistas a futuras adaptaciones del marco jurídico, de apoyar la cooperación y el intercambio de mejores prácticas con las autoridades que intervienen en el espacio controlado de pruebas y de acelerar el acceso a los mercados, también eliminando los obstáculos para las pequeñas y medianas empresas, incluidas las empresas emergentes. Los espacios controlados de pruebas para la IA deben estar ampliamente disponibles en toda la Unión y debe prestarse especial atención a que sean accesibles para las pymes, incluidas las empresas emergentes. La participación en el espacio controlado de pruebas para la IA debe centrarse en cuestiones que generen inseguridad jurídica y que, por lo tanto, dificulten que los proveedores y los proveedores potenciales innoven y experimenten con la IA en la Unión y contribuir a un aprendizaje normativo basado en datos contrastados. Por consiguiente, la supervisión de los sistemas de IA en el espacio controlado de pruebas para la IA debe comprender su desarrollo, entrenamiento, prueba y validación antes de su introducción en el mercado o puesta en servicio, así como el concepto de «modificación sustancial» y su materialización, que puede hacer necesario un nuevo procedimiento de evaluación de la conformidad. Cualquier riesgo significativo detectado durante el proceso de desarrollo y prueba de estos sistemas de IA debe dar lugar a la adopción de medidas de reducción adecuadas y, en su defecto, a la suspensión del proceso de desarrollo y prueba. Cuando proceda, las autoridades nacionales competentes que establezcan espacios controlados de pruebas para la IA deben cooperar con otras autoridades pertinentes, incluidas las que supervisan la protección de los derechos fundamentales, y pueden dar cabida a otros agentes del ecosistema de la IA, como organizaciones de normalización nacionales o europeas, organismos notificados, instalaciones de ensayo y experimentación, laboratorios de investigación y experimentación, centros europeos de innovación digital y organizaciones de partes interesadas y de la sociedad civil pertinentes. Para garantizar una aplicación uniforme en toda la Unión y conseguir economías de escala, resulta oportuno establecer normas comunes para la creación de espacios controlados de pruebas para la IA, así como un marco para la cooperación entre las autoridades pertinentes implicadas en la supervisión de dichos espacios. Los espacios controlados de pruebas para la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otros actos legislativos que permitan el establecimiento de otros espacios controlados de pruebas encaminados a garantizar el cumplimiento de actos legislativos distintos del presente Reglamento. Cuando proceda, las autoridades competentes pertinentes encargadas de esos otros espacios controlados de pruebas deben ponderar las ventajas de utilizarlos también con el fin de garantizar el cumplimiento del presente Reglamento por parte de los sistemas de IA. Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio controlado de pruebas para la IA, las pruebas en condiciones reales también podrán gestionarse y supervisarse en el marco del espacio controlado de pruebas para la IA.

(140) El presente Reglamento debe proporcionar la base jurídica para que los proveedores y los proveedores potenciales en el espacio controlado de pruebas para la IA utilicen datos personales recabados para otros fines para desarrollar determinados sistemas de IA en favor del interés público en el espacio controlado de pruebas para la IA, únicamente en determinadas condiciones, de conformidad con el artículo 6, apartado 4, y el artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y los artículos 5, 6 y 10 del Reglamento (UE) 2018/1725, y sin perjuicio de lo dispuesto en el artículo 4, apartado 2, y el artículo 10 de la Directiva (UE) 2016/680. Siguen siendo aplicables las demás obligaciones de los responsables del tratamiento y los derechos de los interesados en virtud del Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 y la Directiva (UE) 2016/680. En particular, el presente Reglamento no debe ofrecer una base jurídica en el sentido del artículo 22, apartado 2, letra b), del Reglamento (UE) 2016/679 y

del artículo 24, apartado 2, letra b), del Reglamento (UE) 2018/1725. Los proveedores y los proveedores potenciales en el espacio controlado de pruebas para la IA deben proporcionar las garantías adecuadas y cooperar con las autoridades competentes, también siguiendo sus indicaciones y actuando con rapidez y de buena fe para mitigar adecuadamente cualquier riesgo considerable para la seguridad, la salud y los derechos fundamentales que se detecte y pueda surgir durante el desarrollo, las pruebas y la experimentación en dicho espacio.

(141) A fin de acelerar el proceso de desarrollo e introducción en el mercado de los sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento, es importante que los proveedores o proveedores potenciales de dichos sistemas también puedan beneficiarse de un régimen específico para probar dichos sistemas en condiciones reales, sin participar en un espacio controlado de pruebas para la IA. No obstante, en tales casos, teniendo en cuenta las posibles consecuencias de dichas pruebas para las personas físicas, debe garantizarse que el Reglamento establezca garantías y condiciones adecuadas y suficientes para los proveedores o proveedores potenciales. Estas garantías deben incluir, entre otras cosas, la solicitud del consentimiento informado de las personas físicas para participar en pruebas en condiciones reales, salvo en lo que respecta a la garantía del cumplimiento del Derecho cuando intentar obtener el consentimiento informado impediría que se probara el sistema de IA. El consentimiento de los sujetos para participar en tales pruebas en virtud del presente Reglamento es distinto del consentimiento de los interesados para el tratamiento de sus datos personales con arreglo al Derecho pertinente en materia de protección de datos y se entiende sin perjuicio de este. También es importante reducir al mínimo los riesgos y permitir la supervisión por parte de las autoridades competentes y, por tanto, exigir a los proveedores potenciales que presenten a la autoridad de vigilancia del mercado competente un plan de la prueba en condiciones reales, registren la prueba en las secciones específicas de la base de datos de la UE, sin perjuicio de algunas excepciones limitadas, establezcan limitaciones sobre el período durante el que puede llevarse a cabo la prueba y exijan garantías adicionales para las personas pertenecientes a determinados colectivos vulnerables, así como un acuerdo por escrito que defina las funciones y responsabilidades de los proveedores potenciales y de los responsables del despliegue y una supervisión eficaz por parte de personal competente que intervenga en la prueba en condiciones reales. Además, conviene prever garantías adicionales para asegurarse de que sea posible revertir efectivamente y descartar las predicciones, recomendaciones o decisiones del sistema de IA y de que los datos personales se protejan y se supriman cuando los sujetos retiren su consentimiento a participar en la prueba, sin perjuicio de sus derechos como interesados en virtud del Derecho de la Unión en materia de protección de datos. Por lo que respecta a la transferencia de datos, conviene también prever que los datos recopilados y tratados a efectos de las pruebas en condiciones reales solo deben transferirse a terceros países cuando existan garantías adecuadas y aplicables con arreglo al Derecho de la Unión, en particular, de conformidad con las bases para la transferencia de datos personales previstas en el Derecho de la Unión en materia de protección de datos y, en lo referente a los datos no personales, existan garantías adecuadas con arreglo al Derecho de la Unión, como los Reglamentos (UE) 2022/868 ([42]) y (UE) 2023/2854 ([43]) del Parlamento Europeo y del Consejo.

(142) A fin de garantizar que la IA conduzca a resultados positivos desde el punto de vista social y medioambiental, se anima a los Estados miembros a que respalden y promuevan la investigación y el desarrollo de soluciones de IA en apoyo a tales resultados, como soluciones basadas en la IA para aumentar la accesibilidad para las personas con discapacidad, atajar desigualdades socioeconómicas o cumplir los objetivos en materia de medio ambiente, asignando recursos suficientes, incluidos fondos públicos y de la Unión, y, cuando proceda y siempre que se cumplan los criterios de admisibilidad y selección, teniendo en consideración especialmente proyectos que persigan tales objetivos. Dichos proyectos deben basarse en el principio de cooperación interdisciplinaria entre desarrolladores de IA, expertos en desigualdad y no discriminación, en accesibilidad y en derechos del consumidor, medioambientales y digitales, así como representantes del mundo académico.

(143) Para promover y proteger la innovación, es importante tener en particular consideración los intereses de las pymes, incluidas las empresas emergentes, que sean proveedores o responsables del despliegue de sistemas de IA. A tal fin, los Estados miembros deben desarrollar iniciativas en materia de concienciación y comunicación de información, entre otros aspectos, dirigidas a dichos operadores. Los Estados miembros deben proporcionar a las pymes, incluidas las empresas emergentes, que tengan un domicilio social o una sucursal en la Unión, un acceso prioritario a los espacios controlados de pruebas para la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección y sin impedir que otros proveedores y proveedores potenciales accedan a los espacios controlados de pruebas, siempre que se cumplan las mismas condiciones y criterios. Los Estados miembros deben utilizar los canales existentes y establecer, cuando proceda, nuevos canales de comunicación específicos con las pymes, incluidos las empresas emergentes, los responsables del despliegue, otros innovadores y, cuando proceda, las autoridades públicas locales, para apoyar a las pymes durante toda su trayectoria de desarrollo ofreciendo orientaciones y respondiendo a las preguntas sobre la aplicación del presente Reglamento. Cuando proceda, estos canales deben trabajar juntos para crear sinergias y garantizar la homogeneidad de sus orientaciones para las pymes, incluidas las empresas emergentes, y los responsables del despliegue. Además, los Estados miembros deben fomentar la participación de las pymes y otras partes interesadas pertinentes en los procesos de desarrollo de la normalización. Asimismo, los organismos notificados deben tener en cuenta las necesidades y los intereses específicos de los

([42]) Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (DO L 152 de 3.6.2022, p. 1).

([43]) Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

proveedores que sean pymes, incluidas las empresas emergentes, cuando establezcan las tasas aplicables a las evaluaciones de la conformidad. La Comisión debe evaluar periódicamente los costes de la certificación y el cumplimiento para las pymes, incluidas las empresas emergentes, a través de consultas transparentes, y debe trabajar con los Estados miembros para reducir dichos costes. Por ejemplo, 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 particular para los de menor tamaño. En la medida de lo posible, los Estados miembros deben velar por 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 responsables del despliegue transfronterizos. A fin de abordar las necesidades específicas de las pymes, incluidas las empresas emergentes, la Comisión debe proporcionar modelos normalizados para los ámbitos regulados por el presente Reglamento, previa solicitud del Consejo de IA. Además, la Comisión debe complementar los esfuerzos de los Estados miembros proporcionando una plataforma única de información con información fácil de utilizar sobre el presente Reglamento para todos los proveedores y responsables del despliegue, organizando campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento y evaluando y fomentando la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA. Las medianas empresas que hace poco se consideraban pequeñas empresas en el sentido del anexo de la Recomendación 2003/361/CE de la Comisión ([44]) deben tener acceso a esas medidas de apoyo, ya que dichas nuevas medianas empresas a veces pueden carecer de los recursos jurídicos y la formación necesarios para garantizar la comprensión y el cumplimiento adecuados del presente Reglamento.

(144) Con el fin de promover y proteger la innovación, la plataforma de IA a la carta y todos los programas y proyectos de financiación de la Unión pertinentes, como el programa Europa Digital u Horizonte Europa, ejecutados por la Comisión y los Estados miembros a escala nacional o de la Unión deben, cuando proceda, contribuir a la consecución de los objetivos del presente Reglamento.

(145) A fin de 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, en particular las pymes, incluidas las empresas emergentes, y los organismos notificados cumplan las obligaciones que les impone el presente Reglamento, la plataforma de IA a la carta, los centros europeos de innovación digital y las instalaciones de ensayo y experimentación establecidos por la Comisión y los Estados miembros a escala nacional o de la Unión deben contribuir a la aplicación de este Reglamento. En concreto, la plataforma de IA a la carta, los centros europeos de innovación digital y las instalaciones de ensayo y experimentación son capaces de proporcionar a los proveedores y organismos notificados asistencia técnica y científica dentro de sus respectivas misiones y esferas de competencia.

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

(147) Resulta adecuado que la Comisión facilite, en la medida de lo posible, el acceso a las instalaciones de ensayo y experimentación a organismos, grupos o laboratorios establecidos o acreditados con arreglo a la legislación de armonización de la Unión pertinente y que realicen tareas en el marco de la evaluación de la conformidad de productos o dispositivos regulados por dicha legislación. Tal es el caso, en particular, en lo que respecta a los paneles de expertos, los laboratorios especializados y los laboratorios de referencia en el ámbito de los productos sanitarios, de conformidad con los Reglamentos (UE) 2017/745 y (UE) 2017/746.

(148) El presente Reglamento debe establecer un marco de gobernanza que permita tanto coordinar y apoyar su aplicación a escala nacional, como desarrollar capacidades a escala de la Unión e integrar a las partes interesadas en el ámbito de la IA. La aplicación y el cumplimiento efectivos del presente Reglamento requieren un marco de gobernanza que permita coordinar y adquirir conocimientos especializados centrales a escala de la Unión. La Oficina de IA se creó mediante Decisión de la Comisión ([45]) y tiene como misión desarrollar conocimientos especializados y capacidades de la Unión en el ámbito de la IA y contribuir a la aplicación del Derecho de la Unión en materia de IA. Los Estados miembros deben facilitar las tareas de la Oficina de IA con vistas a apoyar el desarrollo de conocimientos especializados y capacidades a escala de la Unión y a fortalecer el funcionamiento del mercado único digital. Además, debe crearse un Consejo de IA compuesto por representantes de los Estados miembros, un grupo de expertos científicos para integrar a la comunidad científica y un foro consultivo para facilitar las aportaciones de las partes interesadas a la aplicación del presente Reglamento, a escala de la Unión y nacional. El desarrollo de conocimientos

([44]) Recomendación 2003/361/CE 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).

([45]) Decisión de la Comisión, de 24 de enero de 2024, por la que se crea la Oficina Europea de Inteligencia Artificial (C/2024/390).

especializados y capacidades de la Unión también debe incluir la utilización de los recursos y conocimientos especializados existentes, en particular a través de sinergias con estructuras creadas en el contexto de la aplicación a escala de la Unión de otros actos legislativos y de sinergias con iniciativas conexas a escala de la Unión, como la Empresa Común EuroHPC y las instalaciones de ensayo y experimentación de IA en el marco del programa Europa Digital.

(149) Debe establecerse un Consejo de IA que facilite la aplicación fluida, efectiva y armonizada del presente Reglamento. El Consejo de IA debe reflejar los diversos intereses del ecosistema de la IA y estar formado por representantes de los Estados miembros. El Consejo de IA debe encargarse de diversas tareas de asesoramiento. Entre otras cosas, debe emitir dictámenes, recomendaciones e informes de asesoramiento o contribuir a orientaciones sobre asuntos relacionados con la aplicación de este Reglamento, también en lo que respecta la ejecución, las especificaciones técnicas o las normas existentes en relación con los requisitos previstos en el presente Reglamento, y asesorar a la Comisión y a los Estados miembros, así como a sus autoridades nacionales competentes, en cuestiones específicas vinculadas a la IA. Con el fin de dar cierta flexibilidad a los Estados miembros en la designación de sus representantes en el Consejo de IA, cualquier persona perteneciente a una entidad pública que tenga las competencias y facultades pertinentes para facilitar la coordinación a escala nacional y contribuir al cumplimiento de las funciones del Consejo de IA podrá ser designada representante. El Consejo de IA debe establecer dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y las autoridades notificantes sobre cuestiones relacionadas, respectivamente, con la vigilancia del mercado y los organismos notificados. El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020. De conformidad con el artículo 33 de dicho Reglamento, la Comisión debe apoyar las actividades del subgrupo permanente de vigilancia del mercado mediante la realización de evaluaciones o estudios de mercado, en particular con vistas a determinar los aspectos del presente Reglamento que requieran una coordinación específica y urgente entre las autoridades de vigilancia del mercado. El Consejo de IA puede establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. El Consejo de IA también debe cooperar, según proceda, con los organismos, grupos de expertos y redes pertinentes de la Unión activos en el contexto del Derecho de la Unión pertinente, incluidos, en particular, los activos en virtud del Derecho de la Unión pertinente en materia de datos y productos y servicios digitales.

(150) Con vistas a garantizar la participación de las partes interesadas en la ejecución y aplicación del presente Reglamento, debe crearse un foro consultivo para asesorar al Consejo de IA y a la Comisión y proporcionarles conocimientos técnicos. A fin de garantizar una representación variada y equilibrada de las partes interesadas que tenga en cuenta los intereses comerciales y no comerciales y, dentro de la categoría de los intereses comerciales, por lo que se refiere a las pymes y otras empresas, el foro consultivo debe incluir, entre otros, a la industria, las empresas emergentes, las pymes, el mundo académico, la sociedad civil, en particular los interlocutores sociales, así como a la Agencia de los Derechos Fundamentales de la Unión Europea, ENISA, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI).

(151) Para apoyar la aplicación y el cumplimiento del presente Reglamento, en particular las actividades de supervisión de la Oficina de IA en lo que respecta a los modelos de IA de uso general, debe crearse un grupo de expertos científicos formado por expertos independientes. Los expertos independientes que constituyan el grupo de expertos científicos deben seleccionarse sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA y deben desempeñar sus funciones con imparcialidad y objetividad y garantizar la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades. A fin de permitir el refuerzo de las capacidades nacionales necesarias para el cumplimiento efectivo del presente Reglamento, los Estados miembros deben poder solicitar el apoyo de los expertos que constituyan el grupo científico para sus actividades de garantía del cumplimiento.

(152) A fin de apoyar una ejecución adecuada en lo que respecta a los sistemas de IA y reforzar las capacidades de los Estados miembros, deben crearse y ponerse a disposición de los Estados miembros estructuras de apoyo a los ensayos de IA de la Unión.

(153) Los Estados miembros desempeñan un papel clave en la aplicación y ejecución del presente Reglamento. En ese sentido, cada Estado miembro debe designar al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Los Estados miembros pueden decidir designar cualquier tipo de entidad pública para que desempeñe las tareas de las autoridades nacionales competentes en el sentido del presente Reglamento, de conformidad con sus características y necesidades organizativas nacionales específicas. Con el fin de incrementar la eficiencia organizativa en los Estados miembros y establecer un único punto de contacto oficial con el público y otros homólogos a escala de los Estados miembros y la Unión, cada Estado miembro debe designar una autoridad de vigilancia del mercado que actúe como punto de contacto único.

(154) Las autoridades nacionales competentes deben ejercer sus poderes de manera independiente, imparcial y objetiva, a fin de preservar los principios de objetividad de sus actividades y funciones y garantizar la aplicación y ejecución del presente Reglamento. Los miembros de estas autoridades deben abstenerse de todo acto incompatible con el carácter de sus funciones y estar sujetos a las normas de confidencialidad establecidas en el presente Reglamento.

(155) Todos los proveedores de sistemas de IA de alto riesgo deben contar con un sistema de vigilancia poscomercialización, 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 que puedan adoptar cualquier medida correctora en el momento oportuno. Cuando proceda, la vigilancia poscomercialización debe incluir un análisis de la interacción con otros sistemas de IA, incluidos otros dispositivos y *software*. La vigilancia poscomercialización no debe comprender los datos operativos sensibles de los responsables del despliegue de sistemas de IA que sean autoridades garantes del cumplimiento del Derecho. Este sistema es también fundamental para garantizar 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, procede exigir a los proveedores que también cuenten con un sistema para comunicar a las autoridades pertinentes cualquier incidente grave asociado al uso de sus sistemas de IA, entendido como un incidente o defecto que tenga como consecuencia un fallecimiento o daños graves para la salud, una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas, el incumplimiento de obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales o daños graves a la propiedad o al medio ambiente.

(156) Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y obligaciones previstos en el presente Reglamento, que constituye legislación de armonización 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. Las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento deben disponer de todos los poderes de ejecución establecidos en el presente Reglamento y en el Reglamento (UE) 2019/1020, y deben ejercer sus poderes y desempeñar sus funciones de manera independiente, imparcial y objetiva. Aunque la mayoría de los sistemas de IA no están sujetos a requisitos ni obligaciones específicos en virtud del presente Reglamento, las autoridades de vigilancia del mercado pueden adoptar medidas en relación con todos los sistemas de IA cuando estos presenten un riesgo de conformidad con el presente Reglamento. Debido a la naturaleza específica de las instituciones, órganos y organismos de la Unión que entran en el ámbito de aplicación del presente Reglamento, procede designar al Supervisor Europeo de Protección de Datos como autoridad de vigilancia del mercado competente para ellos. Esto debe entenderse sin perjuicio de la designación de autoridades nacionales competentes por parte de los Estados miembros. Las actividades de vigilancia del mercado no deben afectar a la capacidad de las entidades supervisadas para llevar a cabo sus tareas de manera independiente, cuando el Derecho de la Unión exija dicha independencia.

(157) El presente Reglamento se entiende sin perjuicio de las competencias, funciones, poderes e independencia de las autoridades u organismos públicos nacionales pertinentes que supervisan la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de igualdad y las autoridades de protección de datos. Cuando sea necesario para su mandato, dichas autoridades u organismos públicos nacionales también deben tener acceso a cualquier documentación creada en virtud del presente Reglamento. Debe establecerse un procedimiento de salvaguardia específico para garantizar una ejecución adecuada y oportuna frente a sistemas de IA que presenten un riesgo para la salud, la seguridad o los derechos fundamentales. El procedimiento relativo a dichos sistemas de IA que presentan un riesgo debe aplicarse a los sistemas de IA de alto riesgo que presenten un riesgo, a los sistemas prohibidos que hayan sido introducidos en el mercado, puestos en servicio o utilizados contraviniendo las prácticas prohibidas establecidas en el presente Reglamento y a los sistemas de IA que hayan sido comercializados infringiendo los requisitos de transparencia establecidos en el presente Reglamento y que presenten un riesgo.

(158) El Derecho de la Unión en materia de 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 los actos jurídicos de la Unión relativos a los servicios financieros, se ha de designar a las autoridades competentes de supervisar y ejecutar dichos actos jurídicos, en particular las autoridades competentes definidas en el Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo ([46]) y las Directivas 2008/48/CE ([47]), 2009/138/CE ([48]),

([46]) Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito, y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013, p. 1).

([47]) Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo (DO L 133 de 22.5.2008, p. 66).

([48]) Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (DO L 335 de 17.12.2009, p. 1).

2013/36/UE ([49]), 2014/17/UE ([50]) y (UE) 2016/97 ([51]) del Parlamento Europeo y del Consejo, dentro de sus respectivas competencias, como las autoridades competentes encargadas de supervisar la aplicación del presente Reglamento, también por lo que respecta a las actividades de vigilancia del mercado, en relación con los sistemas de IA proporcionados o utilizados por las entidades financieras reguladas y supervisadas, a menos que los Estados miembros decidan designar a otra autoridad para que desempeñe estas tareas de vigilancia del mercado. Dichas autoridades competentes deben disponer de todos los poderes previstos en el presente Reglamento y en el Reglamento (UE) 2019/1020 para hacer cumplir los requisitos y obligaciones del presente Reglamento, incluidos los poderes para llevar a cabo actividades de vigilancia del mercado *ex post* que pueden integrarse, en su caso, en sus mecanismos y procedimientos de supervisión existentes en virtud del Derecho pertinente de la Unión en materia de servicios financieros. Conviene prever que, cuando actúen como autoridades de vigilancia del mercado en virtud del presente Reglamento, las autoridades nacionales responsables de la supervisión de las entidades de crédito reguladas por la Directiva 2013/36/UE que participen en el Mecanismo Único de Supervisión establecido por el Reglamento (UE) n.º 1024/2013 del Consejo ([52]) comuniquen sin demora al Banco Central Europeo toda información obtenida en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento. 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, conviene igualmente integrar algunas de las obligaciones procedimentales de los proveedores relativas a la gestión de riesgos, la vigilancia poscomercialización 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 vigilancia impuesta a los responsables del despliegue de sistemas de IA de alto riesgo, en la medida en que estos se apliquen a las entidades de crédito reguladas por la Directiva 2013/36/UE. El mismo régimen debe aplicarse a las empresas de seguros y reaseguros y a las sociedades de cartera de seguros reguladas por la Directiva 2009/138/CE, a los intermediarios de seguros regulados por la Directiva (UE) 2016/97 y a otros tipos de entidades financieras sujetas a requisitos sobre gobernanza, sistemas o procesos internos establecidos con arreglo al Derecho pertinente de la Unión en materia de servicios financieros a fin de garantizar la coherencia y la igualdad de trato en el sector financiero.

(159) Cada autoridad de vigilancia del mercado para los sistemas de IA de alto riesgo en el ámbito de la biometría enumerados en un anexo del presente Reglamento, en la medida en que dichos sistemas se utilicen con fines de garantía del cumplimiento del Derecho, de migración, asilo y gestión del control fronterizo, o de la administración de justicia y los procesos democráticos, debe disponer de facultades de investigación y correctoras efectivas, incluida al menos la facultad de obtener acceso a todos los datos personales que se estén tratando y a toda la información necesaria para el desempeño de sus funciones. Las autoridades de vigilancia del mercado deben poder ejercer sus poderes actuando con total independencia. Cualquier limitación de su acceso a datos operativos sensibles en virtud del presente Reglamento debe entenderse sin perjuicio de los poderes que les confiere la Directiva (UE) 2016/680. Ninguna exclusión de la divulgación de datos a las autoridades nacionales de protección de datos en virtud del presente Reglamento debe afectar a los poderes actuales o futuros de dichas autoridades que trasciendan el ámbito de aplicación del presente Reglamento.

(160) Las autoridades de vigilancia del mercado y la Comisión deben poder proponer actividades conjuntas, incluidas investigaciones conjuntas, que deben llevar a cabo las autoridades de vigilancia del mercado o las autoridades de vigilancia del mercado junto con la Comisión, con el objetivo de fomentar el cumplimiento, detectar incumplimientos, sensibilizar y ofrecer orientaciones en relación con el presente Reglamento con respecto a las categorías específicas de sistemas de IA de alto riesgo que presentan un riesgo grave en dos o más Estados miembros. Tales actividades conjuntas para fomentar el cumplimiento deben llevarse a cabo de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de IA debe prestar apoyo de coordinación a las investigaciones conjuntas.

(161) Es necesario aclarar las responsabilidades y competencias a escala de la Unión y nacional en lo que respecta a los sistemas de IA que se basan en modelos de IA de uso general. Para evitar el solapamiento de competencias, cuando un sistema de IA se base en un modelo de IA de uso general y el modelo y el sistema sean suministrados por el

([49]) 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, 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).

([50]) Directiva 2014/17/UE del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, sobre los contratos de crédito celebrados con los consumidores para bienes inmuebles de uso residencial y por la que se modifican las Directivas 2008/48/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 (DO L 60 de 28.2.2014, p. 34).

([51]) Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros (DO L 26 de 2.2.2016, p. 19).

([52]) Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito (DO L 287 de 29.10.2013, p. 63).

mismo proveedor, la supervisión debe llevarse a cabo a escala de la Unión a través de la Oficina de IA, que debe tener a estos efectos las facultades de una autoridad de vigilancia del mercado en el sentido de lo dispuesto en el Reglamento (UE) 2019/1020. En todos los demás casos, serán responsables de la supervisión de los sistemas de IA las autoridades nacionales de vigilancia del mercado. No obstante, en el caso de los sistemas de IA de uso general que puedan ser utilizados directamente por los responsables del despliegue con al menos un fin clasificado como de alto riesgo, las autoridades de vigilancia del mercado deben cooperar con la Oficina de IA para llevar a cabo evaluaciones de la conformidad e informar de ello al Consejo de IA y a otras autoridades de vigilancia del mercado. Además, las autoridades de vigilancia del mercado deben poder solicitar la asistencia de la Oficina de IA cuando la autoridad de vigilancia del mercado no pueda concluir una investigación sobre un sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA de uso general en el que se basa el sistema de IA de alto riesgo. En tales casos, debe aplicarse *mutatis mutandis* el procedimiento de asistencia mutua transfronteriza previsto en el capítulo VI del Reglamento (UE) 2019/1020.

(162) Para aprovechar al máximo la centralización de conocimientos especializados y las sinergias que se generan a escala de la Unión, deben atribuirse a la Comisión las competencias de supervisión y de control del cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general. La Oficina de IA debe poder llevar a cabo todas las acciones necesarias para supervisar la aplicación efectiva del presente Reglamento en lo que respecta a los modelos de IA de uso general. Debe poder investigar posibles infracciones de las normas relativas a los proveedores de modelos de IA de uso general, tanto por iniciativa propia, a raíz de los resultados de sus actividades de supervisión, como a petición de las autoridades de vigilancia del mercado, de conformidad con las condiciones establecidas en el presente Reglamento. Para promover la eficacia de la supervisión, la Oficina de IA debe prever la posibilidad de que los proveedores posteriores presenten reclamaciones sobre posibles infracciones de las normas relativas a los proveedores de sistemas y modelos de IA de uso general.

(163) Con el fin de complementar los sistemas de gobernanza de los modelos de IA de uso general, el grupo de expertos científicos debe contribuir a las actividades de supervisión de la Oficina de IA y, en determinados casos, puede proporcionar alertas cualificadas a la Oficina de IA que activen actuaciones consecutivas, como investigaciones. Así debe ocurrir cuando el grupo de expertos científicos tenga motivos para sospechar que un modelo de IA de uso general presenta un riesgo concreto e identificable a escala de la Unión. También debe ser este el caso cuando el grupo de expertos científicos tenga motivos para sospechar que un modelo de IA de uso general cumple los criterios que llevarían a clasificarlo como modelo de IA de uso general con riesgo sistémico. A fin de facilitar al grupo de expertos científicos la información necesaria para el desempeño de esas funciones, debe existir un mecanismo que permita al grupo de expertos científicos pedir a la Comisión que solicite documentación o información a un proveedor.

(164) La Oficina de IA debe poder adoptar las medidas necesarias para supervisar la aplicación efectiva y el cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general establecidas en el presente Reglamento. La Oficina de IA debe poder investigar posibles infracciones de conformidad con las competencias previstas en el presente Reglamento, por ejemplo, solicitando documentación e información, realizando evaluaciones y solicitando la adopción de medidas a los proveedores de modelos de IA de uso general. En la realización de las evaluaciones, para poder contar con conocimientos especializados independientes, la Oficina de IA debe poder recurrir a expertos independientes para que lleven a cabo las evaluaciones en su nombre. Se debe poder exigir el cumplimiento de las obligaciones mediante, entre otras cosas, solicitudes de adopción de medidas adecuadas, entre las que se incluyen medidas de reducción del riesgo en caso de que se detecten riesgos sistémicos, así como la restricción de la comercialización, la retirada o la recuperación del modelo. Como salvaguardia, cuando sea necesario, además de los derechos procedimentales previstos en el presente Reglamento, los proveedores de modelos de IA de uso general deben tener los derechos procedimentales previstos en el artículo 18 del Reglamento (UE) 2019/1020, que deben aplicarse *mutatis mutandis*, sin perjuicio de los derechos procesales más específicos previstos en el presente Reglamento.

(165) El desarrollo de sistemas de IA que no sean sistemas de IA de alto riesgo conforme a los requisitos establecidos en el presente Reglamento puede dar lugar a la adopción más amplia de una IA ética y fiable en la Unión. Se debe alentar a los proveedores de sistemas de IA que no son de alto riesgo a crear códigos de conducta, entre los que se incluyen los correspondientes mecanismos de gobernanza, destinados a impulsar la aplicación voluntaria de la totalidad o parte de los requisitos aplicables a los sistemas de IA de alto riesgo, adaptados teniendo en cuenta la finalidad prevista de los sistemas y el menor riesgo planteado y teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector, como las tarjetas de modelo y de datos Asimismo, se debe animar a los proveedores y, en su caso, a los responsables del despliegue de todos los sistemas de IA, ya sean o no de alto riesgo, y de los modelos de IA, a aplicar, con carácter voluntario, requisitos adicionales relativos, por ejemplo, a los elementos de las Directrices éticas de la Unión para una IA fiable, la sostenibilidad medioambiental, medidas de alfabetización en

materia de IA, la inclusividad y la diversidad en el diseño y el desarrollo de los sistemas de IA, lo que incluye tener en cuenta a las personas vulnerables y la accesibilidad de las personas con discapacidad, la participación de las partes interesadas, con la participación, según proceda, de las partes interesadas pertinentes, como las organizaciones empresariales y de la sociedad civil, el mundo académico, los organismos de investigación, los sindicatos y las organizaciones de protección de los consumidores, en el diseño y el desarrollo de los sistemas de IA, y la diversidad de los equipos de desarrollo, también por lo que respecta a la paridad de género. Para garantizar la efectividad de los códigos de conducta voluntarios, estos deben basarse en objetivos claros e indicadores clave del rendimiento que permitan medir la consecución de dichos objetivos. También deben desarrollarse de manera inclusiva, según proceda, con la participación de las partes interesadas pertinentes, como las organizaciones empresariales y de la sociedad civil, el mundo académico, los organismos de investigación, los sindicatos y las organizaciones de protección de los consumidores. La Comisión podría formular iniciativas, también de carácter sectorial, encaminadas a facilitar la disminución de los obstáculos técnicos que dificultan el intercambio transfronterizo de datos para el desarrollo de la IA, también en relación con la infraestructura de acceso a los datos y la interoperabilidad semántica y técnica de distintos tipos de datos.

(166) 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 para los sistemas de IA de alto riesgo 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, el Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo ([53]).

(167) 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, de conformidad con el Derecho de la Unión o nacional, con vistas a garantizar una cooperación fiable y constructiva entre las autoridades competentes a escala de la Unión y nacional. Deben desempeñar sus funciones y actividades de manera que se protejan, en particular, los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales, la aplicación eficaz del presente Reglamento, los intereses de seguridad pública y nacional, la integridad de los procedimientos penales y administrativos y la integridad de la información clasificada.

(168) Se debe poder exigir el cumplimiento del presente Reglamento mediante la imposición de sanciones y otras medidas de ejecución. Los Estados miembros deben tomar todas las medidas necesarias para garantizar que se apliquen las disposiciones del presente Reglamento, también estableciendo sanciones efectivas, proporcionadas y disuasorias para las infracciones, y para respetar el principio de *non bis in idem*. A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, deben establecerse los límites máximos para la imposición de las multas administrativas en el caso de ciertas infracciones concretas. A la hora de determinar la cuantía de las multas, los Estados miembros deben tener en cuenta, en cada caso concreto, todas las circunstancias pertinentes de la situación de que se trate, considerando especialmente la naturaleza, gravedad y duración de la infracción y de sus consecuencias, así como el tamaño del proveedor, en particular si este es una pyme o una empresa emergente. El Supervisor Europeo de Protección de Datos debe estar facultado para imponer multas a las instituciones, los órganos y los organismos de la Unión incluidos en el ámbito de aplicación del presente Reglamento.

(169) Se debe poder exigir el cumplimiento de las obligaciones impuestas en virtud del presente Reglamento a los proveedores de modelos de IA de uso general mediante, entre otras cosas, la imposición de multas. A tal fin, también deben establecerse multas de una cuantía apropiada en caso de incumplimiento de dichas obligaciones, lo que incluye el incumplimiento de las medidas solicitadas por la Comisión de conformidad con el presente Reglamento, con sujeción a los plazos de prescripción pertinentes de conformidad con el principio de proporcionalidad. Todas las decisiones adoptadas por la Comisión en virtud del presente Reglamento están sujetas al control del Tribunal de Justicia de la Unión Europea, de conformidad con lo dispuesto en el TFUE, incluida la competencia jurisdiccional plena del Tribunal de Justicia en materia de sanciones con arreglo al artículo 261 del TFUE.

(170) El Derecho de la Unión y nacional ya prevén vías de recurso efectivas para las personas físicas y jurídicas cuyos derechos y libertades se vean perjudicados por el uso de sistemas de IA. Sin perjuicio de dichas vías de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha producido una infracción del presente Reglamento debe tener derecho a presentar una reclamación ante la autoridad de vigilancia del mercado pertinente.

(171) Las personas afectadas deben tener derecho a obtener una explicación cuando la decisión de un responsable del despliegue se base principalmente en los resultados de salida de determinados sistemas de IA de alto riesgo que entran dentro del ámbito de aplicación del presente Reglamento y cuando dicha decisión produzca efectos jurídicos

([53]) Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (DO L 135 de 23.5.2023, p. 1).

o afecte significativamente de modo similar a dichas personas, de manera que consideren que tiene un efecto negativo en su salud, su seguridad o sus derechos fundamentales. Dicha explicación debe ser clara y significativa y servir de base para que las personas afectadas puedan ejercer sus derechos. El derecho a obtener una explicación no debe aplicarse a la utilización de sistemas de IA para los que se deriven excepciones o restricciones con arreglo al Derecho nacional o de la Unión, y solo debe aplicarse en la medida en que este derecho no esté ya previsto en el Derecho de la Unión.

(172) Las personas que informen sobre infracciones del presente Reglamento deben quedar protegidas por el Derecho de la Unión. Así pues, cuando se informe sobre infracciones del presente Reglamento y en lo que respecta a la protección de las personas que informen sobre dichas infracciones debe aplicarse la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo ([54]).

(173) A fin de garantizar que el marco reglamentario pueda adaptarse cuando sea necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE de modo que pueda modificar las condiciones en las que un sistema de IA no debe considerarse un sistema de alto riesgo, la lista de sistemas de IA de alto riesgo, las disposiciones relativas a la documentación técnica, el contenido de la declaración UE de conformidad, las disposiciones relativas a los procedimientos de evaluación de la conformidad, las disposiciones que establecen 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, el umbral, los parámetros de referencia y los indicadores, lo que incluye la posibilidad de complementar dichos parámetros de referencia e indicadores, de las normas de clasificación de los modelos de IA de uso general con riesgo sistémico, los criterios para clasificar un modelo como modelo de IA de uso general con riesgo sistémico, la documentación técnica para los proveedores de modelos de IA de uso general y la información sobre transparencia para los proveedores de modelos de IA de uso general. 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 de 13 de abril de 2016 sobre la mejora de la legislación ([55]). 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.

(174) Habida cuenta de los rápidos avances tecnológicos y de los conocimientos técnicos necesarios para la aplicación efectiva del presente Reglamento, la Comisión debe evaluar y revisar el presente Reglamento a más tardar el 2 de agosto de 2029 y posteriormente cada cuatro años e informar al Parlamento Europeo y al Consejo. Además, teniendo en cuenta las implicaciones por lo que respecta al ámbito de aplicación del presente Reglamento, la Comisión debe llevar a cabo una evaluación de la necesidad de modificar la lista de sistemas de IA de alto riesgo y la lista de prácticas prohibidas una vez al año. Asimismo, a más tardar 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión debe evaluar y comunicar al Parlamento Europeo y al Consejo la necesidad de modificar la lista de ámbitos de alto riesgo que figura en el anexo del presente Reglamento, los sistemas de IA incluidos en el ámbito de aplicación de las obligaciones de transparencia, la eficacia del sistema de supervisión y gobernanza y los avances en el desarrollo de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general, incluida la necesidad de medidas o acciones adicionales. Por último, a más tardar el 2 de agosto de 2028 y posteriormente cada tres años, la Comisión debe evaluar la repercusión y la eficacia de los códigos de conducta voluntarios para fomentar la aplicación de los requisitos establecidos para los sistemas de IA de alto riesgo a los sistemas de IA que no sean sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para dichos sistemas de IA.

(175) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([56]).

(176) Dado que el objetivo del presente Reglamento, a saber, mejorar el funcionamiento del mercado interior y promover la adopción de una IA centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a sus dimensiones y efectos, pueden lograrse mejor a escala de la Unión, esta puede

([54]) Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (DO L 305 de 26.11.2019, p. 17).
([55]) DO L 123 de 12.5.2016, p. 1.
([56]) 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).

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.

(177) A fin de garantizar la seguridad jurídica, garantizar un período de adaptación adecuado para los operadores y evitar perturbaciones del mercado, también garantizando la continuidad del uso de los sistemas de IA, es conveniente que el presente Reglamento se aplique a los sistemas de IA de alto riesgo que se hayan introducido en el mercado o se hayan puesto en servicio antes de la fecha general de aplicación del Reglamento únicamente si, a partir de esa fecha, dichos sistemas se ven sometidos a cambios significativos en su diseño o su finalidad prevista. Conviene aclarar que, a este respecto, el concepto de «cambio significativo» debe entenderse como equivalente en sustancia al de «modificación sustancial», que se utiliza únicamente con respecto a los sistemas de IA de alto riesgo de conformidad con el presente Reglamento. Con carácter excepcional y a efectos de la rendición pública de cuentas, los operadores de sistemas de IA que sean componentes de sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en un anexo del presente Reglamento y los operadores de sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas deben adoptar, respectivamente, las medidas necesarias para cumplir los requisitos del presente Reglamento antes del final de 2030 y, a más tardar el 2 de agosto de 2030.

(178) Se anima a los proveedores de sistemas de IA de alto riesgo a que empiecen a cumplir, de forma voluntaria, las obligaciones pertinentes del presente Reglamento ya durante el período transitorio.

(179) El presente Reglamento debe aplicarse a partir del 2 de agosto de 2026. No obstante, teniendo en cuenta el riesgo inaceptable asociado a determinadas formas de uso de la IA, las prohibiciones, así como las disposiciones generales del presente Reglamento, deben aplicarse ya desde el 2 de febrero de 2025. Aunque dichas prohibiciones no surtan pleno efecto hasta después del establecimiento de la gobernanza y la aplicación del presente Reglamento, es importante anticipar la aplicación de las prohibiciones para tener en cuenta los riesgos inaceptables y adaptar otros procedimientos, por ejemplo, en el ámbito del Derecho civil. Además, la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad deben estar operativos 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 2 de agosto de 2026. Dada la rápida evolución tecnológica y el elevado ritmo de adopción de modelos de IA de uso general, las obligaciones de los proveedores de modelos de IA de uso general deben aplicarse desde el 2 de agosto de 2025. Los códigos de buenas prácticas deben estar finalizados a más tardar el 2 de mayo de 2025 al objeto de permitir a los proveedores demostrar el cumplimiento de sus obligaciones dentro del plazo previsto. La Oficina de IA debe velar por que las normas y los procedimientos de clasificación estén actualizados con arreglo a los avances tecnológicos. 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. Por lo tanto, las disposiciones relativas a las sanciones deben aplicarse a partir del 2 de agosto de 2025.

(180) El Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos, a los que se consultó de conformidad con el artículo 42, apartados 1 y 2, del Reglamento (UE) 2018/1725, emitieron su dictamen conjunto el 18 de junio de 2021.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

1. El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación.

2. El presente Reglamento establece:

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

b) prohibiciones de determinadas prácticas de IA;

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 determinados sistemas de IA;

e) normas armonizadas para la introducción en el mercado de modelos de IA de uso general;

f) normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento;

g) medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplicará a:

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

b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión;

c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión;

d) los importadores y distribuidores de sistemas de IA;

e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca;

f) los representantes autorizados de los proveedores que no estén establecidos en la Unión;

g) las personas afectadas que estén ubicadas en la Unión.

2. A los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y relativos a productos regulados por los actos legislativos de armonización de la Unión enumerados en la sección B del anexo I, únicamente se les aplicará el artículo 6, apartado 1, y los artículos 102 a 109 y el artículo 112. El artículo 57 se aplicará únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo en virtud del presente Reglamento se hayan integrado en dichos actos legislativos de armonización de la Unión.

3. El presente Reglamento no se aplicará a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias.

El presente Reglamento no se aplicará a los sistemas de IA que, y en la medida en que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

El presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado o no se pongan en servicio en la Unión en los casos en que sus resultados de salida se utilicen en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

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 o de la cooperación internacionales con fines de garantía del cumplimiento del Derecho y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que tal tercer país u organización internacional ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas.

5. El presente Reglamento no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II del Reglamento (UE) 2022/2065.

6. El presente Reglamento no se aplicará a los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad.

7. El Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a los Reglamentos (UE) 2016/679 o (UE) 2018/1725 ni a las Directivas 2002/58/CE o (UE) 2016/680, sin perjuicio del artículo 10, apartado 5, y el artículo 59 del presente Reglamento.

8. El presente Reglamento no se aplicará a ninguna actividad de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Estas actividades se llevarán a cabo de conformidad con el Derecho de la Unión aplicable. Las pruebas en condiciones reales no estarán cubiertas por esa exclusión.

9. El presente Reglamento se entenderá sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores y a la seguridad de los productos.

10. El presente Reglamento no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional.

11. El presente Reglamento no impedirá que la Unión o los Estados miembros mantengan o introduzcan disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores ni que fomenten o permitan la aplicación de convenios colectivos que sean más favorables a los trabajadores.

12. El presente Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto, a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50.

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

2) «riesgo»: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio;

3) «proveedor»: una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;

4) «responsable del despliegue»: una persona física o jurídica, o autoridad pública, órgano u organismo 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»: una persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor;

6) «importador»: una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país;

7) «distribuidor»: una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión;

8) «operador»: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor;

9) «introducción en el mercado»: la primera comercialización en el mercado de la Unión de un sistema de IA o de un modelo de IA de uso general;

10) «comercialización»: el suministro de un sistema de IA o de un modelo de IA de uso general para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, previo pago o gratuitamente;

11) «puesta en servicio»: el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista;

12) «finalidad prevista»: el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, 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, incluidos otros sistemas de IA, razonablemente previsible;

14) «componente de seguridad»: un componente de un producto o un sistema de IA que cumple una función de seguridad para dicho producto o sistema de IA, 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 responsable del despliegue, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA;

16) «recuperación de un sistema de IA»: toda medida encaminada a conseguir la devolución al proveedor de un sistema de IA puesto a disposición de los responsables del despliegue, a inutilizarlo o a desactivar su uso;

17) «retirada de un sistema de IA»: toda medida destinada a impedir la comercialización de un sistema de IA que se encuentra en la cadena de suministro;

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 supervisión;

20) «evaluación de la conformidad»: el proceso por el que se demuestra si se han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo;

21) «organismo de evaluación de la conformidad»: un organismo que desempeña actividades de evaluación de la conformidad de terceros, como el ensayo, la certificación y la inspección;

22) «organismo notificado»: un organismo de evaluación de la conformidad notificado con arreglo al presente Reglamento y a otros actos pertinentes de la legislación de armonización de la Unión;

23) «modificación sustancial»: un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido previsto o proyectado en la evaluación de la conformidad inicial realizada por el proveedor y a consecuencia del cual se vea afectado el cumplimiento por parte del sistema de IA de los requisitos establecidos en el capítulo III, sección 2, o que dé lugar a una modificación de la finalidad prevista para la que se haya evaluado el sistema de IA de que se trate;

24) «marcado CE»: un marcado con el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el capítulo III, sección 2, y con otros actos aplicables de la legislación de armonización de la Unión que prevén su colocación;

25) «sistema de vigilancia poscomercialización»: todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recoger y examinar 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 armonizada tal como se define en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012;

28) «especificación común»: un conjunto de especificaciones técnicas tal como se definen en el artículo 2, punto 4, del Reglamento (UE) n.º 1025/2012 que proporciona medios para cumplir determinados requisitos establecidos en virtud del presente Reglamento;

29) «datos de entrenamiento»: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables;

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 para, entre otras cosas, evitar el subajuste o el sobreajuste;

31) «conjunto de datos de validación»: un conjunto de datos independiente o una parte del conjunto de datos de entrenamiento, obtenida mediante una división fija o variable;

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

33) «datos de entrada»: los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce un resultado de salida;

34) «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, como imágenes faciales o datos dactiloscópicos;

35) «identificación biométrica»: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos;

36) «verificación biométrica»: la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente;

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

38) «datos operativos sensibles»: los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos cuya divulgación podría poner en peligro la integridad de las causas penales;

39) «sistema de reconocimiento de emociones»: un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos;

40) «sistema de categorización biométrica»: un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas;

41) «sistema de identificación biométrica remota»: un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia;

42) «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; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas;

43) «sistema de identificación biométrica remota en diferido»: cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real;

44) «espacio de acceso público»: cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad;

45) «autoridad garante del cumplimiento del Derecho»:

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

b) cualquier otro organismo 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 delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

46) «garantía del cumplimiento del Derecho»: las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

47) «Oficina de IA»: la función de la Comisión consistente en contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y a la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024; las referencias hechas en el presente Reglamento a la Oficina de IA se entenderán hechas a la Comisión;

48) «autoridad nacional competente»: una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos;

49) «incidente grave»: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias:

a) el fallecimiento de una persona o un perjuicio grave para su salud;

b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas;

c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales;

d) daños graves a la propiedad o al medio ambiente;

50) «datos personales»: los datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

51) «datos no personales»: los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

52) «elaboración de perfiles»: la elaboración de perfiles tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679;

53) «plan de la prueba en condiciones reales»: un documento que describe los objetivos, la metodología, el ámbito geográfico, poblacional y temporal, el seguimiento, la organización y la realización de la prueba en condiciones reales;

54) «plan del espacio controlado de pruebas»: un documento acordado entre el proveedor participante y la autoridad competente en el que se describen los objetivos, las condiciones, el calendario, la metodología y los requisitos para las actividades realizadas en el espacio controlado de pruebas;

55) «espacio controlado de pruebas para la IA»: un marco controlado establecido por una autoridad competente que ofrece a los proveedores y proveedores potenciales de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en condiciones reales cuando proceda, un sistema de IA innovador, con arreglo a un plan del espacio controlado de pruebas y durante un tiempo limitado, bajo supervisión regulatoria;

56) «alfabetización en materia de IA»: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar;

57) «prueba en condiciones reales»: la prueba temporal de un sistema de IA para su finalidad prevista en condiciones reales, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar datos sólidos y fiables y evaluar y comprobar la conformidad del sistema de IA con los requisitos del presente Reglamento; si se cumplen todas las condiciones establecidas en el artículo 57 o 60, no se considerará una introducción en el mercado o una puesta en servicio del sistema de IA en el sentido de lo dispuesto en el presente Reglamento;

58) «sujeto»: a los efectos de la prueba en condiciones reales, una persona física que participa en la prueba en condiciones reales;

59) «consentimiento informado»: la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar;

60) «ultrasuplantación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos;

61) «infracción generalizada»: todo acto u omisión contrario al Derecho de la Unión por el que se protegen los intereses de las personas y que:

a) haya perjudicado o pueda perjudicar los intereses colectivos de personas que residen en al menos dos Estados miembros distintos de aquel en el que:

i) se originó o tuvo lugar el acto u omisión,

ii) esté ubicado o establecido el proveedor de que se trate o, en su caso, su representante autorizado, o

iii) esté establecido el responsable del despliegue en el momento de cometer la infracción;

b) haya perjudicado, perjudique o pueda perjudicar los intereses colectivos de las personas y tenga características comunes —incluidas la misma práctica ilícita o la vulneración del mismo interés— y sea cometido simultáneamente por el mismo operador en al menos tres Estados miembros;

62) «infraestructura crítica»: una infraestructura crítica tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2022/2557;

63) «modelo de IA de uso general»: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado;

64) «capacidades de gran impacto»: capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados;

65) «riesgo sistémico»: un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor;

66) «sistema de IA de uso general»: un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA;

67) «operación de coma flotante»: cualquier operación o tarea matemática que implique números de coma flotante, que son un subconjunto de los números reales normalmente representados en los ordenadores mediante un número entero de precisión fija elevado por el exponente entero de una base fija;

68) «proveedor posterior»: un proveedor de un sistema de IA, también de un sistema de IA de uso general, que integra un modelo de IA, con independencia de que el modelo de IA lo proporcione él mismo y esté integrado verticalmente o lo proporcione otra entidad en virtud de relaciones contractuales.

Artículo 4

Alfabetización en materia de IA

Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas.

CAPÍTULO II

PRÁCTICAS DE IA PROHIBIDAS

Artículo 5

Prácticas de IA prohibidas

1. Quedan prohibidas las siguientes prácticas de IA:

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 o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

   i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas 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 de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, 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 víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

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

iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y 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 tendría el uso del sistema en 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 garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), del presente artículo deberá cumplir garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con el Derecho nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.

3. A los efectos del apartado 1, párrafo primero, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. Dicha

autoridad no podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

4. Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

5. 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 garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales 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 y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

6. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho con arreglo al apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado.

7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas.

8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión.

CAPÍTULO III

SISTEMAS DE IA DE ALTO RIESGO

SECCIÓN 1

Clasificación de los sistemas de IA como sistemas de alto riesgo

Artículo 6

Reglas de clasificación de los sistemas de IA de alto riesgo

1. 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), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:

a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y

b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.

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

3. No obstante lo dispuesto en el apartado 2, un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones.

El párrafo primero se aplicará cuando se cumpla cualquiera de las condiciones siguientes:

a) que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada;

b) que el sistema de IA esté destinado a mejorar el resultado de una actividad humana previamente realizada;

c) que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o

d) que el sistema de IA esté destinado a realizar una tarea preparatoria para una evaluación que sea pertinente a efectos de los casos de uso enumerados en el anexo III.

No obstante lo dispuesto en el párrafo primero, los sistemas de IA a que se refiere el anexo III siempre se considerarán de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.

4. El proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto riesgo documentará su evaluación antes de que dicho sistema sea introducido en el mercado o puesto en servicio. Dicho proveedor estará sujeto a la obligación de registro establecida en el artículo 49, apartado 2. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación.

5. La Comisión, previa consulta al Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»), y a más tardar el 2 de febrero de 2026, proporcionará directrices que especifiquen la aplicación práctica del presente artículo en consonancia con el artículo 96, junto con una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, añadiendo nuevas condiciones a las establecidas en dicho apartado, o modificando estas, cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas.

7. La Comisión adoptará actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, suprimiendo cualquiera de las condiciones establecidas en él, cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento.

8. Ninguna modificación de las condiciones establecidas en el apartado 3, párrafo segundo, adoptada de conformidad con los apartados 6 y 7 del presente artículo, reducirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento, y cualquier modificación garantizará la coherencia con los actos delegados adoptados con arreglo al artículo 7, apartado 1, y tendrá en cuenta la evolución tecnológica y del mercado.

Artículo 7

Modificaciones del anexo III

1. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo III mediante la adición o modificación de casos de uso de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) que los sistemas de IA estén destinados a ser utilizados en cualquiera de los ámbitos que figuran en el anexo III, y

b) que los sistemas de IA planteen un riesgo de perjudicar la salud y la seguridad o de tener repercusiones negativas en los derechos fundamentales, y que dicho riesgo sea equivalente a, o mayor que, el riesgo de perjuicio o de repercusiones negativas que plantean los sistemas de IA de alto riesgo que ya se mencionan en el anexo III.

2. Cuando evalúe la condición prevista en el apartado 1, letra b), 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 naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales;

d) el grado de autonomía con el que actúa el sistema de IA y la posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un perjuicio;

e) 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 en los derechos fundamentales o haya dado lugar a problemas importantes en relación con la probabilidad de dicho perjuicio o dichas repercusiones negativas, según demuestren, por ejemplo, los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes o cualquier otro informe, según proceda;

f) 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 varias personas o afectar de manera desproporcionada a un determinado colectivo de personas;

g) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan del resultado generado por un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicho resultado;

h) la medida en que exista un desequilibrio de poder o las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del responsable del despliegue de un sistema de IA, en particular debido a su situación, autoridad, conocimientos, circunstancias económicas o sociales, o edad;

i) la medida en que sea fácil corregir o revertir el resultado generado utilizando un sistema de IA, teniendo en cuenta las soluciones técnicas disponibles para corregirlo o revertirlo y sin que deba considerarse que los resultados que afectan negativamente a la salud, la seguridad o los derechos fundamentales son fáciles de corregir o revertir;

j) la probabilidad de que el despliegue del sistema de IA resulte beneficioso para las personas, los colectivos o la sociedad en general, y la magnitud de este beneficio, incluidas posibles mejoras en la seguridad de los productos;

k) la medida en que el Derecho de la Unión vigente establezca:

   i) vías de recurso efectivas en relación con los riesgos que plantea un sistema de IA, con exclusión de las acciones por daños y perjuicios,

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

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar la lista del anexo III mediante la supresión de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

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

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

SECCIÓN 2

Requisitos de los sistemas de IA de alto riesgo

Artículo 8

Cumplimiento de los requisitos

1. Los sistemas de IA de alto riesgo cumplirán los requisitos establecidos en la presente sección, teniendo en cuenta sus finalidades previstas, así como el estado actual de la técnica generalmente reconocido en materia de IA y tecnologías relacionadas con la IA. A la hora de garantizar el cumplimiento de dichos requisitos se tendrá en cuenta el sistema de gestión de riesgos a que se refiere el artículo 9.

2. Cuando un producto contenga un sistema de IA al que se apliquen los requisitos del presente Reglamento, así como los requisitos de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, los proveedores serán responsables de garantizar que su producto cumpla plenamente todos los requisitos aplicables en virtud de los actos legislativos de armonización de la Unión que sean aplicables. Para garantizar el cumplimiento de los sistemas de IA de alto riesgo a que se refiere el apartado 1 de los requisitos establecidos en la presente sección, y con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los procesos de prueba y presentación de información necesarios, y la información y la documentación que faciliten con respecto a su producto en documentación y procedimientos que ya existan y exijan los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A.

Artículo 9

Sistema de gestión de riesgos

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

2. El sistema de gestión de riesgos se entenderá como un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá revisiones y actualizaciones sistemáticas periódicas. Constará de las siguientes etapas:

a) la determinación y el análisis de los riesgos conocidos y previsibles que el sistema de IA de alto riesgo pueda plantear para la salud, la seguridad o los derechos fundamentales cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista;

b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con 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 vigilancia poscomercialización a que se refiere el artículo 72;

d) la adopción de medidas adecuadas y específicas de gestión de riesgos diseñadas para hacer frente a los riesgos detectados con arreglo a la letra a).

3. Los riesgos a que se refiere el presente artículo son únicamente aquellos que pueden mitigarse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema de IA de alto riesgo o el suministro de información técnica adecuada.

4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), tendrán debidamente en cuenta los efectos y la posible interacción derivados de la aplicación combinada de los requisitos establecidos en la presente sección, con vistas a reducir al mínimo los riesgos de manera más eficaz al tiempo que se logra un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos.

5. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), considerarán aceptables los riesgos residuales pertinentes asociados a cada peligro, así como el riesgo residual general de los sistemas de IA de alto riesgo.

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

a) eliminar o reducir los riesgos detectados y evaluados de conformidad con el apartado 2 en la medida en que sea técnicamente viable mediante un diseño y un desarrollo adecuados del sistema de IA de alto riesgo;

b) implantar, cuando proceda, unas medidas de mitigación y control apropiadas que hagan frente a los riesgos que no puedan eliminarse;

c) proporcionar la información requerida conforme al artículo 13 y, cuando proceda, impartir formación a los responsables del despliegue.

Con vistas a eliminar o reducir los riesgos asociados a la utilización del sistema de IA de alto riesgo, se tendrán debidamente en cuenta los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el responsable del despliegue, así como el contexto en el que está previsto que se utilice el sistema.

6. Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas y específicas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de manera coherente con su finalidad prevista y cumplen los requisitos establecidos en la presente sección.

7. Los procedimientos de prueba podrán incluir pruebas en condiciones reales de conformidad con el artículo 60.

8. 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. Las pruebas se realizarán utilizando parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo.

9. Cuando se implante el sistema de gestión de riesgos previsto en los apartados 1 a 7, los proveedores prestarán atención a si, en vista de su finalidad prevista, es probable que el sistema de IA de alto riesgo afecte negativamente a las personas menores de dieciocho años y, en su caso, a otros colectivos vulnerables.

10. En el caso de los proveedores de sistemas de IA de alto riesgo que estén sujetos a requisitos relativos a procesos internos de gestión de riesgos con arreglo a otras disposiciones pertinentes del Derecho de la Unión, los aspectos previstos en los apartados 1 a 9 podrán formar parte de los procedimientos de gestión de riesgos establecidos con arreglo a dicho Derecho, o combinarse con ellos.

Artículo 10

Datos y gobernanza de datos

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

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, en particular, en lo siguiente:

a) las decisiones pertinentes relativas al diseño;

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

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

d) la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos;

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

f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones;

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

h) la detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecerán de errores y estarán completos en vista de su finalidad prevista. Asimismo, tendrán las propiedades estadísticas adecuadas, por ejemplo, cuando proceda, en lo que respecta a las personas o los colectivos de personas en relación con los cuales está previsto que se utilice el sistema de IA de alto riesgo. Los conjuntos de datos podrán reunir esas características para cada conjunto de datos individualmente o para una combinación de estos.

4. Los conjuntos de datos tendrán en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo.

5. En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, para que se produzca dicho tratamiento deben cumplirse todas las condiciones siguientes:

a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;

b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización;

c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas;

d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos;

e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior;

f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

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

Artículo 11

Documentación técnica

1. La documentación técnica de un sistema de IA de alto riesgo se elaborará antes de su 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 la presente sección y que proporcione de manera clara y completa a las autoridades nacionales competentes y a los organismos notificados la información necesaria para evaluar la conformidad del sistema de IA con dichos requisitos. Contendrá, como mínimo, los elementos contemplados en el anexo IV. Las pymes, incluidas las empresas emergentes, podrán facilitar los elementos de la documentación técnica especificada en el anexo IV de manera simplificada. A tal fin, la Comisión establecerá un formulario simplificado de documentación técnica orientado a las necesidades de las pequeñas empresas y las microempresas. Cuando una pyme, incluidas las empresas emergentes, opte por facilitar la información exigida en el anexo IV de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán dicho formulario a efectos de la evaluación de la conformidad.

2. Cuando se introduzca en el mercado o se ponga en servicio un sistema de IA de alto riesgo asociado a un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión mencionados en el anexo I, sección A, se elaborará un único conjunto de documentos técnicos que contenga toda la información mencionada en el apartado 1, así como la información que exijan dichos actos legislativos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 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 la presente sección.

Artículo 12

Conservación de registros

1. Los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de acontecimientos (en lo sucesivo, «archivos de registro») a lo largo de todo el ciclo de vida del sistema.

2. Para garantizar un nivel de trazabilidad del funcionamiento del sistema de IA de alto riesgo que resulte adecuado para la finalidad prevista del sistema, las capacidades de registro permitirán que se registren acontecimientos pertinentes para:

a) la detección de situaciones que puedan dar lugar a que el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, o a una modificación sustancial;

b) la facilitación de la vigilancia poscomercialización a que se refiere el artículo 72, y

c) la vigilancia del funcionamiento de los sistemas de IA de alto riesgo a que se refiere el artículo 26, apartado 5.

3. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), 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 responsables del despliegue

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones pertinentes previstas en la sección 3.

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 responsables del despliegue.

3. Las instrucciones de uso contendrán al menos la siguiente información:

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

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

   i) su finalidad prevista,

   ii) el nivel de precisión (incluidos los parámetros para medirla), 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, así como cualquier circunstancia conocida y previsible que pueda 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 a que se refiere el artículo 9, apartado 2,

   iv) en su caso, las capacidades y características técnicas del sistema de IA de alto riesgo para proporcionar información pertinente para explicar sus resultados de salida,

v) cuando proceda, su funcionamiento con respecto a determinadas personas o determinados colectivos de personas en relación con los que esté previsto utilizar el sistema,

vi) 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 de alto riesgo,

vii) en su caso, información que permita a los responsables del despliegue interpretar los resultados de salida del sistema de IA de alto riesgo y utilizarla adecuadamente;

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 supervisión humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA de alto riesgo por parte de los responsables del despliegue;

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

f) cuando proceda, una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro de conformidad con el artículo 12.

Artículo 14

Supervisión 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 herramientas de interfaz humano-máquina adecuadas.

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

3. Las medidas de supervisión serán proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo, y se garantizarán bien mediante uno de los siguientes tipos de medidas, bien mediante ambos:

a) las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio;

b) las medidas que el proveedor defina antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el responsable del despliegue.

4. A efectos de la puesta en práctica de lo dispuesto en los apartados 1, 2 y 3, el sistema de IA de alto riesgo se ofrecerá al responsable del despliegue de tal modo que las personas físicas a quienes se encomiende la supervisión humana puedan, según proceda y de manera proporcionada a:

a) entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados;

b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados 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 los resultados de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles;

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

e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura.

5. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las medidas a que se refiere el apartado 3 del presente artículo garantizarán, además, que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación.

El requisito de la verificación por parte de al menos dos personas físicas por separado no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de garantía del cumplimiento del Derecho, de migración, de control fronterizo o de asilo cuando el Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada.

Artículo 15

Precisión, solidez y ciberseguridad

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

2. Para abordar los aspectos técnicos sobre la forma de medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 y cualquier otro parámetro de rendimiento pertinente, la Comisión, en cooperación con las partes interesadas y organizaciones pertinentes, como las autoridades de metrología y de evaluación comparativa, fomentará, según proceda, el desarrollo de parámetros de referencia y metodologías de medición.

3. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión de dichos sistemas, así como los parámetros pertinentes para medirla.

4. Los sistemas de IA de alto riesgo serán lo más resistentes posible en lo que respecta a los errores, fallos o incoherencias que pueden surgir en los propios sistemas o en el entorno en el que funcionan, en particular a causa de su interacción con personas físicas u otros sistemas. Se adoptarán medidas técnicas y organizativas a este respecto.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones 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 se elimine o reduzca lo máximo posible el riesgo de que los resultados de salida que pueden estar sesgados influyan en la información de entrada de futuras operaciones (bucles de retroalimentación) y se garantice que dichos bucles se subsanen debidamente con las medidas de reducción de riesgos adecuadas.

5. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su 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, detectar, combatir, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («envenenamiento de datos»), o los componentes entrenados previamente utilizados en el entrenamiento («envenenamiento de modelos»), la información de entrada diseñada para hacer que el modelo de IA cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo.

SECCIÓN 3

Obligaciones de los proveedores y responsables del despliegue 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 la sección 2;

b) indicarán en el sistema de IA de alto riesgo o, cuando no sea posible, en el embalaje del sistema o en la documentación que lo acompañe, según proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto;

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

d) conservarán la documentación a que se refiere el artículo 18;

e) cuando estén bajo su control, conservarán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 19;

f) se asegurarán de que los sistemas de IA de alto riesgo sean sometidos al procedimiento pertinente de evaluación de la conformidad a que se refiere el artículo 43 antes de su introducción en el mercado o puesta en servicio;

g) elaborarán una declaración UE de conformidad en virtud de lo dispuesto en el artículo 47;

h) colocará el marcado CE en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, para indicar la conformidad con el presente Reglamento, de acuerdo con lo dispuesto en el artículo 48;

i) cumplirán las obligaciones de registro a que se refiere el artículo 49, apartado 1;

j) adoptarán las medidas correctoras necesarias y facilitarán la información exigida en el artículo 20;

k) demostrarán, previa solicitud motivada de la autoridad nacional competente, la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2;

l) velarán por que el sistema de IA de alto riesgo cumpla requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

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 deberá consignarse de manera sistemática y ordenada en documentación en la que se recojan las políticas, los procedimientos y las instrucciones e incluirá, al menos, los siguientes aspectos:

a) una estrategia para el cumplimiento de la normativa, 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 del sistema de IA de alto riesgo y en el control y el aseguramiento de la calidad de este;

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 se ejecutarán;

e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad o no cubran todos los requisitos pertinentes establecidos en la sección 2, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla dichos requisitos;

f) los sistemas y procedimientos de gestión de datos, lo que incluye su adquisición, 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 esa finalidad;

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

h) el establecimiento, aplicación y mantenimiento de un sistema de vigilancia poscomercialización de conformidad con el artículo 72;

i) los procedimientos asociados a la notificación de un incidente grave con arreglo al artículo 73;

j) la gestión de la comunicación con las autoridades nacionales competentes, otras autoridades pertinentes, incluidas las 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 para llevar un registro de toda la documentación e información pertinente;

l) la gestión de los recursos, incluidas medidas relacionadas con la seguridad del 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 aplicación de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor. Los proveedores respetarán, en todo caso, el grado de rigor y el nivel de protección requerido para garantizar la conformidad de sus sistemas de IA de alto riesgo con el presente Reglamento.

3. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o una función equivalente con arreglo al Derecho sectorial pertinente de la Unión podrán incluir los aspectos enumerados en el apartado 1 como parte de los sistemas de gestión de la calidad con arreglo a dicho Derecho.

4. En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de establecer un sistema de gestión de la calidad, salvo en relación con lo dispuesto en el apartado 1, letras g), h) e i), del presente artículo cuando se respeten las normas sobre los sistemas o procesos de gobernanza interna de acuerdo con el Derecho pertinente de la Unión en materia de servicios financieros. A tal fin, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40.

Artículo 18

Conservación de la documentación

1. Durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, 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 47.

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

3. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán la documentación técnica como parte de la documentación conservada en virtud del Derecho pertinente de la Unión en materia de servicios financieros.

Artículo 19

Archivos de registro generados automáticamente

1. Los proveedores de sistemas de IA de alto riesgo conservarán los archivos de registro a que se refiere el artículo 12, apartado 1, que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control. Sin perjuicio del Derecho aplicable de la Unión o nacional, los archivos de registro se conservarán durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que el Derecho de la Unión o nacional aplicable, en particular el Derecho de la Unión en materia de protección de datos personales, disponga otra cosa.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo como parte de la documentación conservada en virtud del Derecho pertinente en materia de servicios financieros.

Artículo 20

Medidas correctoras y obligación de información

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

2. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, y el proveedor tenga conocimiento de dicho riesgo, este investigará inmediatamente las causas, en colaboración con el responsable del despliegue que lo haya notificado, en su caso, e informará a las autoridades de vigilancia del mercado competentes respecto al sistema de IA de alto riesgo de que se trate y, cuando proceda, al organismo notificado que haya expedido un certificado para dicho sistema de conformidad con lo dispuesto en el artículo 44, en particular sobre la naturaleza del incumplimiento y sobre cualquier medida correctora adoptada.

Artículo 21

Cooperación con las autoridades competentes

1. Los proveedores de sistemas de IA de alto riesgo, previa solicitud motivada de una autoridad competente, proporcionarán a dicha autoridad toda la información y la documentación necesarias para demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, en una lengua que la autoridad pueda entender fácilmente y que sea una de las lenguas oficiales de las instituciones de la Unión, indicada por el Estado miembro de que se trate.

2. Previa solicitud motivada de una autoridad competente, los proveedores darán también a dicha autoridad, cuando proceda, acceso a los archivos de registro generados automáticamente del sistema de IA de alto riesgo a que se refiere el artículo 12, apartado 1, en la medida en que dichos archivos estén bajo su control.

3. Toda información obtenida por una autoridad competente con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 22

Representantes autorizados de los proveedores de sistemas de IA de alto riesgo

1. Antes de comercializar sus sistemas de IA de alto riesgo en el mercado de la Unión, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.

3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a las autoridades de vigilancia del mercado, cuando lo soliciten, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión según lo indicado por la autoridad de competente. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) verificar que se han elaborado la declaración UE de conformidad a que se refiere el artículo 47 y la documentación técnica a que se refiere el artículo 11 y que el proveedor ha llevado a cabo un procedimiento de evaluación de la conformidad adecuado;

b) conservar a disposición de las autoridades competentes y de las autoridades u organismos nacionales a que se refiere el artículo 74, apartado 10, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, los datos de contacto del proveedor que haya nombrado al representante autorizado, una copia de la declaración UE de conformidad a que se refiere el artículo 47, la documentación técnica y, en su caso, el certificado expedido por el organismo notificado;

c) proporcionar a una autoridad competente, previa solicitud motivada, toda la información y la documentación, incluida la mencionada en el presente párrafo, letra b), que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, incluido el acceso a los archivos de registro a que se refiere el artículo 12, apartado 1, generados automáticamente por ese sistema, en la medida en que dichos archivos estén bajo el control del proveedor;

d) cooperar con las autoridades competentes, previa solicitud motivada, en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que este presente;

e) cuando proceda, cumplir las obligaciones de registro a que se refiere el artículo 49, apartado 1, o si el registro lo lleva a cabo el propio proveedor, garantizar que la información a que se refiere el anexo VIII, sección A, punto 3, es correcta.

El mandato habilitará al representante autorizado para que las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

4. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene las obligaciones que le atañen con arreglo al presente Reglamento. En tal caso, además, informará de inmediato de la terminación del mandato y de los motivos de esta medida a la autoridad de vigilancia del mercado pertinente, así como, cuando proceda, al organismo notificado pertinente.

Artículo 23

Obligaciones de los importadores

1. Antes de introducir un sistema de IA de alto riesgo en el mercado, los importadores se asegurarán de que el sistema sea conforme con el presente Reglamento verificando que:

a) el proveedor del sistema de IA de alto riesgo haya llevado a cabo el procedimiento de evaluación de la conformidad pertinente a que se refiere el artículo 43;

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

c) el sistema lleve el marcado CE exigido y vaya acompañado de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso;

d) el proveedor haya designado a un representante autorizado de conformidad con el artículo 22, apartado 1.

2. Si el importador tiene motivos suficientes para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, ha sido falsificado o va acompañado de documentación falsificada, no lo introducirá en el mercado hasta que se haya conseguido la conformidad de dicho sistema. Si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79, apartado 1, el importador informará de ello al proveedor del sistema, a los representantes autorizados y a las autoridades de vigilancia del mercado.

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

4. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometan el cumplimiento de los requisitos establecidos en la sección 2 por parte de dicho sistema.

5. Los importadores conservarán, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, una copia del certificado expedido por el organismo notificado, en su caso, de las instrucciones de uso y de la declaración UE de conformidad a que se refiere el artículo 47.

6. Los importadores proporcionarán a las autoridades competentes pertinentes, previa solicitud motivada, toda la información y la documentación, incluidas las referidas en el apartado 5, que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 en una lengua que estas puedan entender fácilmente. A tal efecto, velarán asimismo por que la documentación técnica pueda ponerse a disposición de esas autoridades.

7. Los importadores cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo introducido en el mercado por los importadores, en particular para reducir y mitigar los riesgos que este presente.

Artículo 24

Obligaciones de los distribuidores

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores verificarán que este lleve el marcado CE exigido, que vaya acompañado de una copia de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso, y que el proveedor y el importador de dicho sistema, según corresponda, hayan cumplido sus obligaciones establecidas en el artículo 16, letras b) y c), y el artículo 23, apartado 3, respectivamente.

2. Si un distribuidor considera o tiene motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en la sección 2, no lo comercializará hasta que se haya conseguido esa conformidad. Además, si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79, 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 de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometen el cumplimiento por parte del sistema de los requisitos establecidos en la sección 2.

4. Los distribuidores que consideren o tengan motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo que han comercializado no es conforme con los requisitos establecidos en la sección 2 adoptarán las medidas correctoras necesarias para que sea conforme, para 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 79, apartado 1, su distribuidor informará inmediatamente de ello al proveedor o al importador del sistema y a las autoridades competentes respecto al sistema de IA de alto riesgo de que se trate y dará detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

5. Previa solicitud motivada de una autoridad competente pertinente, los distribuidores de un sistema de IA de alto riesgo proporcionarán a esa autoridad toda la información y la documentación relativas a sus actuaciones con arreglo a los apartados 1 a 4 que sean necesarias para demostrar que dicho sistema cumple los requisitos establecidos en la sección 2.

6. Los distribuidores cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo comercializado por los distribuidores, en particular para reducir o mitigar los riesgos que este presente.

Artículo 25

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

1. Cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor de un sistema de IA de alto riesgo 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 ponga su nombre o marca en un sistema de IA de alto riesgo previamente introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo;

b) cuando modifique sustancialmente un sistema de IA de alto riesgo que ya haya sido introducido en el mercado o puesto en servicio de tal manera que siga siendo un sistema de IA de alto riesgo con arreglo al artículo 6;

c) cuando modifique la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido considerado de alto riesgo y ya haya sido introducido en el mercado o puesto en servicio, de tal manera que el sistema de IA de que se trate se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

2. Cuando se den las circunstancias mencionadas en el apartado 1, el proveedor que inicialmente haya introducido en el mercado el sistema de IA o lo haya puesto en servicio dejará de ser considerado proveedor de ese sistema de IA específico a efectos del presente Reglamento. Ese proveedor inicial cooperará estrechamente con los nuevos proveedores y facilitará la información necesaria, el acceso técnico u otra asistencia razonablemente previstos que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo. El presente apartado no se aplicará en los casos en que el proveedor inicial haya indicado claramente que su sistema de IA no debe ser transformado en un sistema de IA de alto riesgo y, por lo tanto, no está sujeto a la obligación de facilitar la documentación.

3. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos contemplados en los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el fabricante del producto será considerado proveedor del sistema de IA de alto riesgo y estará sujeto a las obligaciones previstas en el artículo 16 en alguna de las siguientes circunstancias:

a) que el sistema de IA de alto riesgo se introduzca en el mercado junto con el producto bajo el nombre o la marca del fabricante del producto;

b) que el sistema de IA de alto riesgo se ponga en servicio bajo el nombre o la marca del fabricante del producto después de que el producto haya sido introducido en el mercado.

4. El proveedor de un sistema de IA de alto riesgo y el tercero que suministre un sistema de IA de alto riesgo, herramientas, servicios, componentes o procesos que se utilicen o integren en un sistema de IA de alto riesgo especificarán, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y otra asistencia que sean necesarios, sobre la base del estado de la técnica generalmente reconocido, para que el proveedor del sistema de IA de alto riesgo pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento. El presente apartado no se aplicará a terceros que pongan a disposición del público herramientas, servicios, procesos o componentes distintos de modelos de IA de uso general, en el marco de una licencia libre y de código abierto.

La Oficina de IA podrá elaborar y recomendar cláusulas contractuales tipo, de carácter voluntario, entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en los sistemas de IA de alto riesgo. Cuando elabore esas cláusulas contractuales tipo de carácter voluntario, la Oficina de IA tendrá en cuenta los posibles requisitos contractuales aplicables en determinados sectores o modelos de negocio. Las cláusulas contractuales tipo de carácter voluntario se publicarán y estarán disponibles gratuitamente en un formato electrónico fácilmente utilizable.

5. Los apartados 2 y 3 se entenderán sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales, de conformidad con el Derecho de la Unión y nacional.

Artículo 26

Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo

1. Los responsables del despliegue de sistemas de IA de alto riesgo adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen, de acuerdo con los apartados 3 y 6.

2. Los responsables del despliegue encomendarán la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

3. Las obligaciones previstas en los apartados 1 y 2 no afectan a otras obligaciones que el Derecho nacional o de la Unión imponga a los responsables del despliegue ni a su libertad para organizar sus propios recursos y actividades con el fin de poner en práctica las medidas de supervisión humana que indique el proveedor.

4. Sin perjuicio de lo dispuesto en los apartados 1 y 2, el responsable del despliegue se asegurará de que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos.

5. Los responsables del despliegue vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso y, cuando proceda, informarán a los proveedores con arreglo al artículo 72. Cuando los responsables del despliegue tengan motivos para considerar que utilizar el sistema de IA de alto riesgo conforme a sus instrucciones puede dar lugar a que ese sistema de AI presente un riesgo en el sentido del artículo 79, apartado 1, informarán, sin demora indebida, al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente y suspenderán el uso de ese sistema. Cuando los responsables del despliegue detecten un incidente grave, informarán asimismo inmediatamente de dicho incidente, en primer lugar, al proveedor y, a continuación, al importador o distribuidor y a la autoridad de vigilancia del mercado pertinente. En el caso de que el responsable del despliegue no consiga contactar con el proveedor, el artículo 73 se aplicará *mutatis mutandis*. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue de sistemas de IA que sean autoridades garantes del cumplimiento del Derecho.

En el caso de los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de vigilancia prevista en el párrafo primero cuando se respeten las normas sobre sistemas, procesos y mecanismos de gobernanza interna de acuerdo con el Derecho pertinente en materia de servicios financieros.

6. Los responsables del despliegue 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, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que se disponga otra cosa en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.

Los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro como parte de la documentación conservada en virtud del Derecho de la Unión en materia de servicios financieros.

7. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empleadores informarán a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo. Esta información se facilitará, cuando proceda, con arreglo a las normas y procedimientos establecidos en el Derecho de la Unión y nacional y conforme a las prácticas en materia de información a los trabajadores y sus representantes.

8. Los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas o instituciones, órganos y organismos de la Unión cumplirán las obligaciones de registro a que se refiere el artículo 49. Cuando dichos responsables del despliegue constaten que el sistema de IA de alto riesgo que tienen previsto utilizar no ha sido registrado en la base de datos de la UE a que se refiere el artículo 71, no utilizarán dicho sistema e informarán al proveedor o al distribuidor.

9. Cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo utilizarán la información facilitada conforme al artículo 13 del presente Reglamento 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.

10. No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, *ex ante* o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

En caso de que se deniegue la autorización contemplada en el párrafo primero, dejará de utilizarse el sistema de identificación biométrica remota en diferido objeto de la solicitud de autorización con efecto inmediato y se eliminarán los datos personales asociados al uso del sistema de IA de alto riesgo para el que se solicitó la autorización.

Dicho sistema de IA de alto riego de identificación biométrica remota en diferido no se utilizará en ningún caso a los efectos de la garantía del cumplimiento del Derecho de forma indiscriminada, sin que exista relación alguna con un delito, un proceso penal, una amenaza real y actual o real y previsible de delito, o con la búsqueda de una persona desaparecida concreta. Se velará por que las autoridades garantes del cumplimiento del Derecho no puedan adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida de dichos sistemas de identificación biométrica remota en diferido.

El presente apartado se entiende sin perjuicio del artículo 9 del Reglamento (UE) 2016/679 y del artículo 10 de la Directiva (UE) 2016/680 para el tratamiento de los datos biométricos.

Con independencia de la finalidad o del responsable del despliegue, se documentará toda utilización de tales sistemas de IA de alto riesgo en el expediente policial pertinente y se pondrá a disposición, previa solicitud, de la autoridad de vigilancia del mercado pertinente y de la autoridad nacional de protección de datos, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. El presente párrafo se entenderá sin perjuicio de los poderes conferidas por la Directiva (UE) 2016/680 a las autoridades de control.

Los responsables del despliegue presentarán informes anuales a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos sobre el uso que han hecho de los sistemas de identificación biométrica remota en diferido, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. Los informes podrán agregarse de modo que cubran más de un despliegue.

Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota en diferido.

11. Sin perjuicio de lo dispuesto en el artículo 50 del presente Reglamento, los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas informarán a las personas físicas de que están expuestas a la utilización de los sistemas de IA de alto riesgo. En el caso de los sistemas de IA de alto riesgo que se utilicen a los efectos de la garantía del cumplimiento del Derecho, se aplicará el artículo 13 de la Directiva (UE) 2016/680.

12. Los responsables del despliegue cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo con el objetivo de aplicar el presente Reglamento.

Artículo 27

Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo

1. Antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales. A tal fin, los responsables del despliegue llevarán a cabo una evaluación que consistirá en:

a) una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista;

b) una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;

c) las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;

d) los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13;

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

f) las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

2. La obligación descrita con arreglo al apartado 1 se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si, durante el uso del sistema de IA de alto riesgo, el responsable del despliegue considera que alguno de los elementos enumerados en el apartado 1 ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información.

3. Una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado, presentando el modelo cumplimentado a que se refiere el apartado 5 del presente artículo. En el caso contemplado en el artículo 46, apartado 1, los responsables del despliegue podrán quedar exentos de esta obligación de notificación.

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

5. La Oficina de IA elaborará un modelo de cuestionario, también mediante una herramienta automatizada, a fin de facilitar que los responsables del despliegue cumplan sus obligaciones en virtud del presente artículo de manera simplificada.

SECCIÓN 4

Autoridades notificantes y organismos notificados

Artículo 28

Autoridades notificantes

1. Cada Estado miembro nombrará o constituirá al menos 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 supervisión. Dichos procedimientos se desarrollarán por medio de la cooperación entre las autoridades notificantes de todos los Estados miembros.

2. Los Estados miembros podrán decidir que la evaluación y la supervisión contempladas en el apartado 1 sean realizadas por un organismo nacional de acreditación en el sentido del Reglamento (CE) n.º 765/2008 y con arreglo a este.

3. Las autoridades notificantes se constituirán, se organizarán y funcionarán de forma que no surjan conflictos de intereses 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 consultoría de carácter comercial o competitivo.

6. Las autoridades notificantes preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

7. Las autoridades notificantes dispondrán de suficiente personal competente para efectuar adecuadamente sus tareas. Cuando proceda, el personal competente tendrá los conocimientos especializados necesarios para ejercer sus funciones, en ámbitos como las tecnologías de la información, la IA y el Derecho, incluida la supervisión de los derechos fundamentales.

Artículo 29

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 los tipos de sistemas de IA en relación con los 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 31.

Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante en virtud de cualquier otro acto de la 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 periódicamente que cumple los requisitos establecidos en el artículo 31.

4. En lo que respecta a los organismos notificados designados de conformidad con cualquier otro acto legislativo 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. El organismo notificado actualizará la documentación a que se refieren los apartados 2 y 3 del presente artículo cuando se produzcan cambios pertinentes, para que la autoridad responsable de los organismos notificados pueda supervisar y verificar que se siguen cumpliendo todos los requisitos establecidos en el artículo 31.

Artículo 30

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 31.

2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros, mediante el sistema de notificación electrónica desarrollado y gestionado por la Comisión, cada organismo de evaluación de la conformidad a que se refiere el apartado 1.

3. La notificación a que se refiere el apartado 2 del presente artículo incluirá información detallada de las actividades de evaluación de la conformidad, el módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA afectados, así como la certificación de competencia pertinente. Si la notificación no está basada en el certificado de acreditación a que se refiere el artículo 29, apartado 2, la autoridad notificante facilitará a la Comisión y a los demás Estados miembros las pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones existentes destinadas a garantizar que se supervisará periódicamente al organismo y que este continuará satisfaciendo los requisitos establecidos en el artículo 31.

4. El organismo de evaluación de la conformidad de que se trate 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 dos semanas tras la notificación de una autoridad notificante cuando esta incluya el certificado de acreditación a que se refiere el artículo 29, apartado 2, o de dos meses tras la notificación de la autoridad notificante cuando esta incluya las pruebas documentales a que se refiere el artículo 29, apartado 3.

5. Cuando se formulen objeciones, la Comisión iniciará sin demora consultas con los Estados miembros pertinentes y el organismo de evaluación de la conformidad. En vista de todo ello, la Comisión enviará su decisión al Estado miembro afectado y al organismo de evaluación de la conformidad pertinente.

Artículo 31

Requisitos relativos a los organismos notificados

1. Los organismos notificados se establecerán de conformidad con el Derecho nacional de los Estados miembros y tendrán personalidad jurídica.

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

3. La estructura organizativa, la distribución de las responsabilidades, la línea jerárquica y el funcionamiento de los organismos notificados ofrecerán confianza en su 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 los sistemas de IA de alto riesgo que se evalúen, así como de cualquier competidor del proveedor. Ello no será óbice para el uso de sistemas de IA de alto riesgo evaluados que sean necesarios para las actividades del organismo de evaluación de la conformidad o para el uso de tales sistemas de alto riesgo con fines personales.

5. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, el desarrollo, la comercialización o el uso de dichos sistemas de IA de alto riesgo, ni tampoco representarán a las partes que llevan a cabo estas actividades. Además, no efectuarán ninguna actividad que pudiera entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que han sido notificados. Ello se aplicará especialmente a los servicios de consultoría.

6. 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 poner en práctica los principios de imparcialidad aplicables en toda su organización, a todo su personal y en todas sus actividades de evaluación.

7. Los organismos notificados contarán con procedimientos documentados que garanticen que su personal, sus comités, sus filiales, sus subcontratistas y todos sus organismos asociados o personal de organismos externos mantengan, de conformidad con el artículo 78, la confidencialidad de la información que llegue a su poder en el desempeño de las actividades de evaluación de la conformidad, excepto en aquellos casos en que la ley exija su divulgación. 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 funciones que les hayan sido encomendadas en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que desarrollen sus actividades.

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

9. Los organismos notificados suscribirán un seguro de responsabilidad adecuado para sus actividades de evaluación de la conformidad, salvo que la responsabilidad la asuma el Estado miembro en que estén establecidos con arreglo al Derecho nacional o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

10. Los organismos notificados serán capaces de llevar a cabo todas sus tareas 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.

11. Los organismos notificados contarán con competencias técnicas internas suficientes para poder evaluar de manera eficaz las tareas que lleven a cabo agentes externos en su nombre. El organismo notificado dispondrá permanentemente de suficiente personal administrativo, técnico, jurídico y científico que tenga experiencia y conocimientos relativos a los tipos de sistemas de IA, los datos y la computación de datos pertinentes y a los requisitos establecidos en la sección 2.

12. 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 pertinentes.

Artículo 32

Presunción de conformidad con los requisitos relativos a los organismos notificados

Cuando un organismo de evaluación de la conformidad demuestre que cumple los criterios establecidos en las normas armonizadas pertinentes, o en partes de estas, cuyas referencias estén publicadas en el *Diario Oficial de la Unión Europea*, se presumirá que cumple los requisitos establecidos en el artículo 31 en la medida en que las normas armonizadas aplicables contemplen esos mismos requisitos.

Artículo 33

Filiales de organismos notificados y subcontratación

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 31 e informará a la autoridad notificante en consecuencia.

2. Los organismos notificados asumirán la plena responsabilidad de las tareas realizadas por cualesquiera subcontratistas o filiales.

3. Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del proveedor. Los organismos notificados pondrán a disposición del público una lista de sus filiales.

4. Los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial y el trabajo que estos realicen en virtud del presente Reglamento se mantendrán a disposición de la autoridad notificante durante un período de cinco años a partir de la fecha de finalización de la subcontratación.

Artículo 34

Obligaciones operativas de los 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 establecidos en el artículo 43.

2. Los organismos notificados evitarán cargas innecesarias para los proveedores cuando desempeñen sus actividades, y tendrán debidamente en cuenta el tamaño del proveedor, el sector en que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate, en particular con vistas a reducir al mínimo las cargas administrativas y los costes del cumplimiento para las microempresas y pequeñas empresas en el sentido de la Recomendación 2003/361/CE. El organismo notificado respetará, sin embargo, el grado de rigor y el nivel de protección requeridos para que el sistema de IA de alto riesgo cumpla los requisitos del presente Reglamento.

3. Los organismos notificados pondrán a disposición de la autoridad notificante mencionada en el artículo 28, y le presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, a fin de que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión, y de facilitar la evaluación descrita en la presente sección.

Artículo 35

Números de identificación y listas de organismos notificados

1. La Comisión asignará un número de identificación único a cada organismo notificado, incluso cuando un organismo sea notificado con arreglo a más de un acto de la Unión.

2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, incluidos sus números de identificación 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. La autoridad notificante notificará a la Comisión y a los demás Estados miembros cualquier cambio pertinente en la notificación de un organismo notificado a través del sistema de notificación electrónica a que se refiere el artículo 30, apartado 2.

2. Los procedimientos establecidos en los artículos 29 y 30 se aplicarán a las ampliaciones del ámbito de aplicación de la notificación.

Para modificaciones de la notificación distintas de las ampliaciones de su ámbito de aplicación, se aplicarán los procedimientos establecidos en los apartados 3 a 9.

3. Cuando un organismo notificado decida poner fin a sus actividades de evaluación de la conformidad, informará de ello a la autoridad notificante y a los proveedores afectados tan pronto como sea posible y, cuando se trate de un cese planeado, al menos un año antes de poner fin a sus actividades. Los certificados del organismo notificado podrán seguir siendo válidos durante un plazo de nueve meses después del cese de las actividades del organismo notificado, siempre que otro organismo notificado haya confirmado por escrito que asumirá la responsabilidad de los sistemas de IA de alto riesgo cubiertos por dichos certificados. Este último organismo notificado realizará una evaluación completa de los sistemas de IA de alto riesgo afectados antes del vencimiento de ese plazo de nueve meses y antes de expedir nuevos certificados para esos sistemas. Si el organismo notificado ha puesto fin a sus actividades, la autoridad notificante retirará la designación.

4. Si una autoridad notificante tiene motivo suficiente para considerar que un organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, la autoridad notificante investigará el asunto sin demora y 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 ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, dicha autoridad limitará, suspenderá o retirará la designación, según el caso, dependiendo de la gravedad del incumplimiento de dichos requisitos u obligaciones. Asimismo, informará de ello inmediatamente a la Comisión y a los demás Estados miembros.

5. Cuando su designación haya sido suspendida, limitada o retirada total o parcialmente, el organismo notificado informará a los proveedores afectados a más en un plazo de diez días.

6. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante adoptará las medidas oportunas para garantizar que los archivos del organismo notificado de que se trate se conserven, y para ponerlos a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado, a petición de estas.

7. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante:

a) evaluará las repercusiones en los certificados expedidos por el organismo notificado;

b) presentará a la Comisión y a los demás Estados miembros un informe con sus conclusiones en un plazo de tres meses a partir de la notificación de los cambios en la designación;

c) exigirá al organismo notificado que suspenda o retire, en un plazo razonable determinado por la autoridad, todo certificado indebidamente expedido, a fin de garantizar la conformidad continua de los sistemas de IA de alto riesgo en el mercado;

d) informará a la Comisión y a los Estados miembros de los certificados cuya suspensión o retirada haya exigido;

e) facilitará a las autoridades nacionales competentes del Estado miembro en el que el proveedor tenga su domicilio social toda la información pertinente sobre los certificados cuya suspensión o retirada haya exigido; dicha autoridad tomará las medidas oportunas, cuando sea necesario, para evitar un riesgo para la salud, la seguridad o los derechos fundamentales.

8. Salvo en el caso de los certificados expedidos indebidamente, y cuando una designación haya sido suspendida o limitada, los certificados mantendrán su validez en una de las circunstancias siguientes:

a) cuando, en el plazo de un mes a partir de la suspensión o la limitación, la autoridad notificante haya confirmado que no existe riesgo alguno para la salud, la seguridad o los derechos fundamentales en relación con los certificados afectados por la suspensión o la limitación y haya fijado un calendario de acciones para subsanar la suspensión o la limitación, o

b) cuando la autoridad notificante haya confirmado que no se expedirán, modificarán ni volverán a expedir certificados relacionados con la suspensión mientras dure la suspensión o limitación, y declare si el organismo notificado tiene o no la capacidad, durante el período de la suspensión o limitación, de seguir supervisando los certificados expedidos y siendo responsable de ellos; cuando la autoridad notificante determine que el organismo notificado no tiene la capacidad de respaldar los certificados expedidos, el proveedor del sistema cubierto por el certificado deberá confirmar por escrito a las autoridades nacionales competentes del Estado miembro en que tenga su domicilio social, en un plazo de tres meses a partir de la suspensión o limitación, que otro organismo notificado cualificado va a asumir temporalmente las funciones del organismo notificado para supervisar los certificados y ser responsable de ellos durante el período de la suspensión o limitación.

9. Salvo en el caso de los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados mantendrán su validez durante nueve meses en las circunstancias siguientes:

a) la autoridad nacional competente del Estado miembro en el que tiene su domicilio social el proveedor del sistema de IA de alto riesgo cubierto por el certificado ha confirmado que no existe ningún riesgo para la salud, la seguridad o los derechos fundamentales asociado al sistema de IA de alto riesgo de que se trate, y

b) otro organismo notificado ha confirmado por escrito que asumirá la responsabilidad inmediata de dichos sistemas de IA y completa su evaluación en el plazo de doce meses a partir de la retirada de la designación.

En las circunstancias a que se refiere el párrafo primero, la autoridad nacional competente del Estado miembro en el que tenga su domicilio social el proveedor del sistema cubierto por el certificado podrá prorrogar la validez provisional de los certificados por plazos adicionales de tres meses, sin exceder de doce meses en total.

La autoridad nacional competente o el organismo notificado que asuman las funciones del organismo notificado afectado por el cambio de la designación informarán de ello inmediatamente a la Comisión, a los demás Estados miembros y a los demás organismos notificados.

Artículo 37

Cuestionamiento 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 la competencia de un organismo notificado o del cumplimiento continuo, por parte de un organismo notificado, de los requisitos establecidos en el artículo 31 y de sus responsabilidades aplicables.

2. La autoridad notificante facilitará a la Comisión, a petición de esta, toda la información pertinente relativa a la notificación o el mantenimiento de la competencia del organismo notificado de que se trate.

3. La Comisión garantizará el tratamiento confidencial de acuerdo con el artículo 78 de toda la información delicada recabada en el transcurso de sus investigaciones en virtud del presente artículo.

4. Cuando la Comisión determine que un organismo notificado no cumple o ha dejado de cumplir los requisitos para su notificación, informará al Estado miembro notificante en consecuencia y le solicitará que adopte las medidas correctoras necesarias, incluidas la suspensión o la retirada de la designación en caso necesario. Si el Estado miembro no adopta las medidas correctoras necesarias, la Comisión, mediante un acto de ejecución, podrá suspender, limitar o retirar la designación. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

Artículo 38

Coordinación de los organismos notificados

1. La Comisión se asegurará de que se instaure y se mantenga convenientemente, en relación con los sistemas de IA de alto riesgo, una adecuada coordinación y cooperación entre los organismos notificados activos en los procedimientos de evaluación de la conformidad en virtud del presente Reglamento, en forma de grupo sectorial de organismos notificados.

2. Cada autoridad notificante se asegurará de que los organismos notificados por ella participen en el trabajo del grupo a que se refiere el apartado 1, directamente o por medio de representantes designados.

3. La Comisión dispondrá que se organicen intercambios de conocimientos y mejores prácticas entre autoridades notificantes.

Artículo 39

Organismos de evaluación de la conformidad de terceros países

Los organismos de evaluación de la conformidad establecidos en virtud del Derecho de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados a desempeñar las actividades de los organismos notificados con arreglo al presente Reglamento, siempre que cumplan los requisitos establecidos en el artículo 31 o garanticen un nivel equivalente de cumplimiento.

SECCIÓN 5

Normas, evaluación de la conformidad, certificados, registro

Artículo 40

Normas armonizadas y documentos de normalización

1. Los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con normas armonizadas, o partes de estas, cuyas referencias estén publicadas en el *Diario Oficial de la Unión Europea* de conformidad con el Reglamento (UE) n.º 1025/2012 se presumirá que son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, en su caso, con las obligaciones establecidas en el capítulo V, secciones 2 y 3, del presente Reglamento, en la medida en que dichas normas contemplen estos requisitos u obligaciones.

2. De conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, la Comisión formulará, sin demora indebida, peticiones de normalización que contemplen todos los requisitos establecidos en la sección 2 del presente capítulo y, según proceda, las peticiones de normalización que contemplen las obligaciones establecidas en el capítulo V, secciones 2 y 3, del presente Reglamento. La petición de normalización también incluirá la solicitud de documentos sobre los procesos de presentación de información y documentación a fin de mejorar el funcionamiento de los de los sistemas de IA desde el punto de vista de los recursos, como la reducción del consumo de energía y de otros recursos del sistema de IA de alto riesgo durante su ciclo de vida, así como sobre el desarrollo eficiente desde el punto de vista energético de los modelos de IA de uso general. Cuando prepare una petición de normalización, la Comisión consultará al Consejo de IA y a las partes interesadas pertinentes, incluido el foro consultivo.

Cuando dirija una petición de normalización a las organizaciones europeas de normalización, la Comisión especificará que las normas deben ser claras, coherentes —también con las normas elaboradas en diversos sectores para los productos regulados por los actos legislativos de armonización de la Unión vigentes enumerados en el anexo I— y destinadas a garantizar que los sistemas de IA de alto riesgo o los modelos de IA de uso general introducidos en el mercado o puestos en servicio en la Unión cumplan los requisitos u obligaciones pertinentes establecidos en el presente Reglamento.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de que han hecho todo lo posible por cumplir los objetivos a que se refieren los párrafos primero y segundo del presente apartado, de conformidad con el artículo 24 del Reglamento (UE) n.º 1025/2012.

3. Los participantes en el proceso de normalización tratarán de promover la inversión y la innovación en IA, también incrementando la seguridad jurídica, así como la competitividad y el crecimiento del mercado de la Unión, de contribuir al refuerzo de la cooperación mundial en pro de la normalización, teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que son coherentes con los valores, derechos fundamentales e intereses de la Unión, y de mejorar la gobernanza multilateral, garantizando una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) n.º 1025/2012.

Artículo 41

Especificaciones comunes

1. La Comisión podrá adoptar actos de ejecución por los que se establezcan especificaciones comunes para los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, siempre que se hayan cumplido las siguientes condiciones:

a) la Comisión ha solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en la sección 2 del presente capítulo, o según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, y:

   i) la solicitud no ha sido aceptada por ninguna de las organizaciones europeas de normalización, o

ii) las normas armonizadas que responden a dicha solicitud no se han entregado en el plazo establecido de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, o

iii) las normas armonizadas pertinentes responden de forma insuficiente a las preocupaciones en materia de derechos fundamentales, o

iv) las normas armonizadas no se ajustan a la solicitud, y

b) no se ha publicado en el *Diario Oficial de la Unión Europea* ninguna referencia a normas armonizadas que regulen los requisitos establecidos en la sección 2 del presente capítulo, o según proceda, las obligaciones a que se refiere el capítulo V, secciones 2 y 3, de conformidad con el Reglamento (UE) n.º 1025/2012 y no se prevé la publicación de tal referencia en un plazo razonable.

Al elaborar las disposiciones comunes, la Comisión consultará al foro consultivo a que se refiere el artículo 67.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 98, apartado 2.

2. Antes de elaborar un proyecto de acto de ejecución, la Comisión informará al comité a que se refiere el artículo 22 del Reglamento (UE) n.º 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 1 del presente artículo.

3. Se presumirá que los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con las especificaciones comunes a que se refiere el apartado 1, o partes de dichas especificaciones, son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para cumplir con las obligaciones a que se refiere el capítulo V, secciones 2 y 3, en la medida en que dichas especificaciones comunes contemplen esos requisitos o esas obligaciones.

4. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el *Diario Oficial de la Unión Europea*, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.º 1025/2012. Cuando la referencia a una norma armonizada se publique en el *Diario Oficial de la Unión Europea*, la Comisión derogará los actos de ejecución a que se refiere el apartado 1, o las partes de dichos actos que contemplen los mismos requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, las mismas obligaciones establecidas en el capítulo V, secciones 2 y 3.

5. Cuando los proveedores de sistemas de IA de alto riesgo o los modelos de IA de uso general no cumplan las especificaciones comunes mencionadas en el apartado 1, justificarán debidamente que han adoptado soluciones técnicas que cumplan los requisitos a que se refiere la sección 2 del presente capítulo o, según corresponda, cumplan con las obligaciones establecidas en el capítulo V, secciones 2 y 3, en un nivel como mínimo equivalente a aquellos.

6. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en la sección 2, o, según corresponda, no cumple con las obligaciones establecidas en el capítulo V, secciones 2 y 3, informará de ello a la Comisión con una explicación detallada. La Comisión evaluará dicha información y, en su caso, modificará el acto de ejecución por el que se establece la especificación común de que se trate.

Artículo 42

Presunción de conformidad con determinados requisitos

1. Se presumirá que los sistemas de IA de alto riesgo que hayan sido entrenados y probados con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto su uso cumplen los requisitos pertinentes establecidos en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo que cuenten con un certificado o una declaración de conformidad en virtud de un esquema de ciberseguridad con arreglo al Reglamento (UE) 2019/881 cuyas referencias estén publicadas 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, contemplen dichos requisitos.

Artículo 43

Evaluación de la conformidad

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

a) el fundamentado en el control interno, mencionado en el anexo VI, o

b) el 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.

Al demostrar el cumplimiento de los requisitos establecidos en la sección 2 por parte de un sistema de IA de alto riesgo, el proveedor se atendrá al procedimiento de evaluación de la conformidad establecido en el anexo VII cuando:

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

b) el proveedor no haya aplicado la norma armonizada, o solo haya aplicado parte de esta;

c) existan las especificaciones comunes a que se refiere la letra a), pero el proveedor no las haya aplicado;

d) una o varias de las normas armonizadas a que se refiere la letra a) se hayan publicado con una limitación, y únicamente en la parte de la norma objeto de la limitación.

A efectos del procedimiento de evaluación de la conformidad mencionado en el anexo VII, el proveedor podrá escoger cualquiera de los organismos notificados. No obstante, cuando se prevea la puesta en servicio del sistema de IA de alto riesgo por parte de las autoridades garantes del cumplimiento del Derecho, las autoridades de inmigración o las autoridades de asilo, o por las instituciones, órganos u organismos de la Unión, la autoridad de vigilancia del mercado mencionada en el artículo 74, apartado 8 o 9, según proceda, actuará como organismo notificado.

2. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, 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.

3. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el proveedor se atendrá al procedimiento de evaluación de la conformidad pertinente exigida por dichos actos legislativos. Los requisitos establecidos en la sección 2 del presente capítulo 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 y 4.5 del anexo VII, así como el punto 4.6, párrafo quinto, de dicho anexo.

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 la sección 2, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 31, apartados 4, 5, 10 y 11, en el contexto del procedimiento de notificación con arreglo a dichos actos legislativos.

Cuando un acto legislativo enumerado en el anexo I, sección A, permita al fabricante del producto prescindir de una evaluación de la conformidad de terceros, a condición de que el fabricante haya aplicado todas las normas armonizadas que contemplan todos los requisitos pertinentes, dicho fabricante solamente podrá recurrir a esta opción si también ha aplicado las normas armonizadas o, en su caso, las especificaciones comunes a que se refiere el artículo 41 que contemplan todos los requisitos establecidos en la sección 2 del presente capítulo.

4. Los sistemas de IA de alto riesgo que ya hayan sido objeto de un procedimiento de evaluación de la conformidad se someterán a un nuevo procedimiento de evaluación de la conformidad en caso de modificación sustancial, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el responsable del despliegue 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 en la información recogida en la documentación técnica mencionada en el anexo IV, punto 2, letra f), no constituirán modificaciones sustanciales.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar los anexos VI y VII actualizándolos a la luz del progreso técnico.

6. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar los apartados 1 y 2 del presente artículo a fin de someter a los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, 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 mencionado 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 los organismos notificados con arreglo al anexo VII se redactarán en una lengua que las autoridades pertinentes del Estado miembro en el que esté establecido el organismo notificado puedan entender fácilmente.

2. Los certificados serán válidos para el período que indiquen, que no excederá de cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III. A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales no superiores a cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables. Todo suplemento de un certificado mantendrá su validez a condición de que el certificado al que complementa sea válido.

3. Si un organismo notificado observa que un sistema de IA ya no cumple los requisitos establecidos en la sección 2, 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.

Existirá un procedimiento de recurso frente a las decisiones de los organismos notificados, también respecto a los certificados de conformidad expedidos.

Artículo 45

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, de cualquier suplemento a dichos certificados y de cualesquiera aprobaciones de sistemas de gestión de la calidad expedidas con arreglo a los requisitos establecidos 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 expedida con arreglo a los requisitos establecidos en el anexo VII;

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

d) de cualquier 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 aplicación de su notificación y de cualquier otra actividad realizada, incluidas 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 gestión de la calidad que haya expedido;

b) de los certificados de la Unión de evaluación de la documentación técnica 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 los mismos tipos de sistemas de IA información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de las evaluaciones de la conformidad.

4. Los organismos notificados preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

Artículo 46

Exención del procedimiento de evaluación de la conformidad

1. Como excepción a lo dispuesto en el artículo 43 y previa solicitud debidamente motivada, cualquier autoridad de vigilancia del mercado podrá autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo específicos en el territorio del Estado miembro de que se trate por motivos excepcionales de seguridad pública o con el fin de proteger la vida y la salud de las personas, el medio ambiente o activos fundamentales de la industria y de las infraestructuras. Dicha autorización se concederá por un período limitado, mientras se lleven a cabo los procedimientos de evaluación de la conformidad necesarios, teniendo en cuenta los motivos excepcionales que justifiquen la exención. La conclusión de los procedimientos de que se trate se alcanzará sin demora indebida.

2. En una situación de urgencia debidamente justificada por motivos excepcionales de seguridad pública o en caso de amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas, las autoridades garantes del cumplimiento del Derecho o las autoridades de protección civil podrán poner en servicio un sistema de IA de alto riesgo específico sin la autorización a que se refiere el apartado 1, siempre que se solicite dicha autorización durante o después de la utilización sin demora indebida. Si se deniega la autorización a que se refiere el apartado 1, se suspenderá el uso del sistema de IA de alto riesgo con efecto inmediato y se desecharán inmediatamente todos los resultados y toda la información de salida producidos por dicho uso.

3. 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 la sección 2. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida de conformidad con los apartados 1 y 2. Esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho.

4. Si, en el plazo de quince días naturales tras la recepción de la información indicada en el apartado 3, 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.

5. Si, en el plazo de quince días naturales tras la recepción de la notificación a que se refiere el apartado 3, 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 3 es infundada, la Comisión celebrará consultas con el Estado miembro pertinente sin demora. Se consultará a los 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 a los operadores pertinentes.

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

7. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, solo se aplicarán las exenciones de la evaluación de la conformidad establecidas en dichos actos legislativos de armonización de la Unión.

Artículo 47

Declaración UE de conformidad

1. El proveedor redactará una declaración UE de conformidad por escrito en un formato legible por máquina, con firma electrónica o manuscrita, para cada sistema de IA de alto riesgo y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años a contar desde la introducción del sistema de IA de alto riesgo en el mercado o su puesta en servicio. En la declaración UE de conformidad se especificará el sistema de IA de alto riesgo para el que ha sido redactada. Se entregará 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 establecidos en la sección 2. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a una lengua que puedan entender fácilmente las autoridades nacionales competentes del Estado o Estados miembros en que se introduzca en el mercado o comercialice el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sujetos a otros actos legislativos de armonización de la Unión que también exijan una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a todos el Derecho de la Unión aplicable al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para determinar los actos legislativos de armonización de la Unión a los que se refiere la declaración.

4. Al elaborar la declaración UE de conformidad, el proveedor asumirá la responsabilidad del cumplimiento de los requisitos establecidos en la sección 2. El proveedor mantendrá actualizada la declaración UE de conformidad según proceda.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo V actualizando el contenido de la declaración UE de conformidad establecida en dicho anexo, con el fin de introducir elementos que resulten necesarios a la luz del progreso técnico.

Artículo 48

Marcado CE

1. El marcado CE estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008.

2. En el caso de los sistemas de IA de alto riesgo que se proporcionan digitalmente, se utilizará un marcado CE digital, únicamente si es fácilmente accesible a través de la interfaz desde la que se accede a dicho sistema o mediante un código fácilmente accesible legible por máquina u otros medios electrónicos.

3. 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.

4. 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 del organismo notificado lo colocará él mismo o, siguiendo sus instrucciones, el proveedor o el representante autorizado del proveedor. 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.

5. Cuando los sistemas de IA de alto riesgo estén sujetos a otras disposiciones del Derecho de la Unión que también requieran la colocación del marcado CE, este indicará que los sistemas de IA de alto riesgo también cumplen los requisitos de esas otras disposiciones.

Artículo 49

Registro

1. Antes de introducir en el mercado o de poner en servicio un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, el proveedor o, en su caso, el representante autorizado, registrarán su sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

2. Antes de introducir en el mercado o poner en servicio un sistema de IA sobre el que el proveedor haya llegado a la conclusión de que no es de alto riesgo de conformidad con el artículo 6, apartado 3, dicho proveedor o, en su caso, el representante autorizado, registrarán ese sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

3. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos de la UE a que se refiere el artículo 71.

4. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, el registro a que se refieren los apartados 1, 2 y 3 del presente artículo se efectuará en una sección segura no pública de la base de datos de la UE a que se refiere el artículo 71 e incluirá únicamente la información, según proceda, a la que se hace referencia en:

a) el anexo VIII, sección A, puntos 1 a 10, con excepción de los puntos 6, 8 y 9;

b) el anexo VIII, sección B, puntos 1 a 5 y puntos 8 y 9;

c) el anexo VIII, sección C, puntos 1 a 3;

d) el anexo IX, puntos 1, 2, 3 y 5.

Únicamente la Comisión y las autoridades nacionales a que se refiere el artículo 74, apartado 8, tendrán acceso a las secciones restringidas respectivas de la base de datos de la UE enumeradas en el párrafo primero del presente apartado.

5. Los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, se registrarán a nivel nacional.

CAPÍTULO IV

OBLIGACIONES DE TRANSPARENCIA DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE DETERMINADOS SISTEMAS DE IA

Artículo 50

Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de forma que las personas físicas de que se trate estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar un delito penal.

2. Los proveedores de sistemas de IA, entre los que se incluyen los sistemas de IA de uso general, que generen contenido sintético de audio, imagen, vídeo o texto, velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial. Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica, o cuando estén autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos.

3. Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él y tratarán sus datos personales de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y con la Directiva (UE) 2016/680, según corresponda. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones que hayan sido autorizados por ley para detectar, prevenir e investigar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la Unión.

4. Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial. Esta obligación no se aplicará cuando la ley autorice su uso para para detectar, prevenir, investigar o enjuiciar delitos. Cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra.

Los responsables del despliegue de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público divulgarán que el texto se ha generado o manipulado de manera artificial. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar o enjuiciar delitos, o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido.

5. La información a que se refieren los apartados 1 a 4 se facilitará a las personas físicas de que se trate de manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición. La información se ajustará a los requisitos de accesibilidad aplicables.

6. Los apartados 1 a 4 no afectarán a los requisitos y obligaciones establecidos en el capítulo III y se entenderán sin perjuicio de otras obligaciones de transparencia establecidas en el Derecho nacional o de la Unión para los responsables del despliegue de sistemas de IA.

7. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión para promover la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados de manera artificial. La Comisión podrá adoptar actos de ejecución a fin de aprobar dichos códigos de buenas prácticas, de conformidad con el procedimiento establecido en el artículo 56, apartado 6. Si considera que el código no es adecuado, la Comisión podrá adoptar un acto de ejecución que especifique normas comunes para el cumplimiento de las citadas obligaciones de conformidad con el procedimiento de examen establecido en el artículo 98, apartado 2.

CAPÍTULO V

MODELOS DE IA DE USO GENERAL

SECCIÓN 1

Reglas de clasificación

Artículo 51

Reglas de clasificación de los modelos de IA de uso general como modelos de IA de uso general con riesgo sistémico

1. Un modelo de IA de uso general se clasificará como modelo de IA de uso general con riesgo sistémico si reúne alguna de las siguientes condiciones:

a) tiene capacidades de gran impacto evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia;

b) con arreglo a una decisión de la Comisión, adoptada de oficio o a raíz de una alerta cualificada del grupo de expertos científicos, tiene capacidades o un impacto equivalente a los establecidos en la letra a), teniendo en cuenta los criterios establecidos en el anexo XIII.

2. Se presumirá que un modelo de IA de uso general tiene capacidades de gran impacto con arreglo al apartado 1, letra a), cuando la cantidad acumulada de cálculo utilizada para su entrenamiento, medida en operaciones de coma flotante, sea superior a 10^{25}.

3. La Comisión adoptará actos delegados de conformidad con el artículo 97 para modificar los umbrales a que se refieren los apartados 1 y 2 del presente artículo, así como para complementar los parámetros de referencia e indicadores en función de los avances tecnológicos, como las mejoras algorítmicas o la mayor eficiencia del hardware, cuando sea necesario, para que los umbrales reflejen el estado actual de la técnica.

Artículo 52

Procedimiento

1. Cuando un modelo de IA de uso general cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), el proveedor pertinente lo notificará a la Comisión sin demora y, en cualquier caso, antes de transcurridas dos semanas desde que se cumpla dicho requisito o desde que se sepa que va a cumplirse. Dicha notificación incluirá la información necesaria para demostrar que se cumple el requisito pertinente. Si la Comisión tiene conocimiento de un modelo de IA de uso general que presenta riesgos sistémicos y que no ha sido notificado, podrá decidir designarlo como modelo con riesgo sistémico.

2. El proveedor de un modelo de IA de uso general que cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), podrá presentar, junto con su notificación, argumentos suficientemente fundamentados que demuestren que, excepcionalmente, aunque el modelo de IA de uso general cumple dicho requisito, no presenta riesgos sistémicos, debido a sus características específicas, y no debe clasificarse, por tanto, como modelo de IA de uso general con riesgo sistémico.

3. Cuando la Comisión concluya que los argumentos presentados con arreglo al apartado 2 no están suficientemente fundamentados y que el proveedor pertinente no ha sido capaz de demostrar que el modelo de IA de uso general no presenta, debido a sus características específicas, riesgos sistémicos, rechazará dichos argumentos y el modelo de IA de uso general se considerará un modelo de IA de uso general con riesgo sistémico.

4. La Comisión podrá determinar que un modelo de IA de uso general presenta riesgos sistémicos, de oficio o a raíz de una alerta cualificada del grupo de expertos científicos con arreglo al artículo 90, apartado 1, letra a), a partir de los criterios establecidos en el anexo XIII.

La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar el anexo XIII especificando y actualizando los criterios establecidos en dicho anexo.

5. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de uso general con riesgo sistémico con arreglo al apartado 4, la Comisión tendrá en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de uso general presenta riesgos sistémicos con arreglo a los criterios establecidos en el anexo XIII. Dicha solicitud contendrá motivos objetivos, detallados y nuevos que hayan surgido desde la decisión de designación. Los proveedores no podrán solicitar la reevaluación antes de transcurridos seis meses desde la decisión de designación. Si tras la reevaluación la Comisión decide mantener la designación como modelo de IA de uso general con riesgo sistémico, los proveedores no podrán solicitar otra reevaluación hasta transcurridos seis meses desde dicha decisión.

6. La Comisión velará por que se publique una lista de modelos de IA de uso general con riesgo sistémico, que mantendrá actualizada, sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

SECCIÓN 2

Obligaciones de los proveedores de modelos de IA de uso general

Artículo 53

Obligaciones de los proveedores de modelos de IA de uso general

1. Los proveedores de modelos de IA de uso general:

a) elaborarán y mantendrán actualizada la documentación técnica del modelo, incluida la información relativa al proceso de entrenamiento y realización de pruebas y los resultados de su evaluación, que contendrá, como mínimo, la información establecida en el anexo XI con el fin de facilitarla, previa solicitud, a la Oficina de IA y a las autoridades nacionales competentes;

b) elaborarán y mantendrán actualizada información y documentación y la pondrán a disposición de los proveedores de sistemas de IA que tengan la intención de integrar el modelo de IA de uso general en sus sistemas de IA. Sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional, dicha información y documentación:

   i) permitirá a los proveedores de sistemas de IA entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones en virtud del presente Reglamento, y

   ii) contendrá, como mínimo, los elementos previstos en el anexo XII;

c) establecerán directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines, y en particular, para detectar y cumplir, por ejemplo, a través de tecnologías punta, una reserva de derechos expresada de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790;

d) elaborarán y pondrán a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA.

2. Las obligaciones establecidas en el apartado 1, letras a) y b), no se aplicarán a los proveedores de modelos de IA que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Esta excepción no se aplicará a los modelos de IA de uso general con riesgo sistémico.

3. Los proveedores de modelos de IA de uso general cooperarán con la Comisión y las autoridades nacionales competentes, según sea necesario, en el ejercicio de sus competencias y facultades en virtud del presente Reglamento.

4. Los proveedores de modelos de IA de uso general podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

5. A fin de facilitar el cumplimiento de lo dispuesto en el anexo XI, en particular en su punto 2, letras d) y e), la Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 para detallar las metodologías de medición y cálculo con vistas a que la documentación sea comparable y verificable.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97, apartado 2, para modificar los anexos XI y XII en función de los avances tecnológicos.

7. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 54

Representantes autorizados de los proveedores de modelos de IA de uso general

1. Antes de introducir en el mercado de la Unión un modelo de IA de uso general, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.

3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a la Oficina de IA, cuando lo solicite, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) comprobar que se ha elaborado la documentación técnica que se indica en el anexo XI y que el proveedor cumple todas las obligaciones a que se refiere el artículo 53 y, en su caso, el artículo 55;

b) conservar una copia de la documentación técnica que se indica en el anexo XI a disposición de la Oficina de IA y de las autoridades nacionales competentes por un período de diez años a partir de la introducción en el mercado del modelo de IA de uso general, y de los datos de contacto del proveedor que haya designado al representante autorizado;

c) facilitar a la Oficina de IA, previa solicitud motivada, toda la información y documentación, incluidas la información y documentación mencionadas en la letra b), que sean necesarias para demostrar el cumplimiento de las obligaciones establecidas en el presente capítulo;

d) cooperar con la Oficina de IA y las autoridades competentes, previa solicitud motivada, en cualquier acción que emprendan en relación con el modelo de IA de uso general, también cuando el modelo esté integrado en un sistema de IA introducido en el mercado o puesto en servicio en la Unión.

4. El mandato habilitará al representante autorizado para que la Oficina de IA o las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

5. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene sus obligaciones en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la Oficina de IA del fin del mandato y de los motivos para ello.

6. La obligación establecida en el presente artículo no se aplicará a los proveedores de modelos de IA de uso general que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, salvo si los citados modelos de IA de uso general presentan riesgos sistémicos.

SECCIÓN 3

Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico

Artículo 55

Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico

1. Además de las obligaciones enumeradas en los artículos 53 y 54, los proveedores de modelos de IA de uso general con riesgo sistémico:

a) evaluarán los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, lo que incluye la realización y documentación de pruebas de simulación de adversarios con el modelo con vistas a detectar y mitigar riesgos sistémicos;

b) evaluarán y mitigarán los posibles riesgos sistémicos a escala de la Unión que puedan derivarse del desarrollo, la introducción en el mercado o el uso de modelos de IA de uso general con riesgo sistémico, así como el origen de dichos riesgos;

c) vigilarán, documentarán y comunicarán, sin demora indebida, a la Oficina de IA y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctoras para resolverlos;

d) velarán por que se establezca un nivel adecuado de protección de la ciberseguridad para el modelo de IA de uso general con riesgo sistémico y la infraestructura física del modelo.

2. Los proveedores de modelos de IA de uso general con riesgo sistémico podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

3. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

SECCIÓN 4

Códigos de buenas prácticas

Artículo 56

Códigos de buenas prácticas

1. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión a fin de contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta los planteamientos internacionales.

2. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas comprendan al menos las obligaciones establecidas en los artículos 53 y 55, entre las que se incluyen las cuestiones siguientes:

a) los medios para garantizar que la información a que se refiere el artículo 53, apartado 1, letras a) y b), se mantenga actualizada con respecto a la evolución del mercado y los avances tecnológicos;

b) el nivel adecuado de detalle por lo que respecta al resumen sobre el contenido utilizado para el entrenamiento;

c) la determinación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluido su origen, cuando proceda;

d) las medidas, procedimientos y modalidades de evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación, que serán proporcionales a los riesgos y tendrán en cuenta su gravedad y probabilidad y las dificultades específicas para hacerles frente, habida cuenta de la manera en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA.

3. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general, así como a las autoridades nacionales competentes pertinentes, a participar en la elaboración de códigos de buenas prácticas. Las organizaciones de la sociedad civil, la industria, el mundo académico y otras partes interesadas pertinentes, como los proveedores posteriores y los expertos independientes, podrán contribuir al proceso.

4. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas establezcan claramente sus objetivos específicos y contengan compromisos o medidas, como, por ejemplo, indicadores clave de rendimiento, si procede, para garantizar la consecución de dichos objetivos, y que tengan debidamente en cuenta las necesidades e intereses de todas las partes interesadas, incluidas las personas afectadas, a escala de la Unión.

5. La Oficina de IA velará por que los participantes en los códigos de buenas prácticas informen periódicamente a la Oficina de IA sobre la aplicación de los compromisos y las medidas adoptadas y sus resultados, lo que incluye su evaluación con respecto a los indicadores clave de rendimiento, si procede. Los indicadores clave de rendimiento y los compromisos de presentación de información reflejarán las diferencias de tamaño y capacidad entre los distintos participantes.

6. La Oficina de IA y el Consejo de IA supervisarán y evaluarán periódicamente la consecución de los objetivos de los códigos de buenas prácticas por parte de los participantes y su contribución a la correcta aplicación del presente Reglamento. La Oficina de IA y el Consejo de IA evaluarán si los códigos de buenas prácticas incluyen las obligaciones establecidas en los artículos 53 y 55, y supervisarán y evaluarán periódicamente la consecución de sus objetivos. Publicarán su evaluación de la adecuación de los códigos de buenas prácticas.

La Comisión podrá, mediante un acto de ejecución, aprobar un código de buenas prácticas y conferirle una validez general dentro de la Unión. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

7. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general a adherirse a los códigos de buenas prácticas. En el caso de los proveedores de modelos de IA de uso general que no presenten riesgos sistémicos, esta adhesión podrá limitarse a las obligaciones previstas en el artículo 53, salvo que declaren expresamente su interés en adherirse al código completo.

8. La Oficina de IA también fomentará y facilitará, según proceda, la revisión y la adaptación de los códigos de buenas prácticas, en particular teniendo en cuenta las normas emergentes. La Oficina de IA asistirá en la evaluación de las normas disponibles.

9. Los códigos de buenas prácticas estarán finalizados a más tardar el 2 de mayo de 2025. La Oficina de IA adoptará las medidas necesarias, lo que incluye invitar a los proveedores a adherirse a los códigos de buenas prácticas con arreglo a lo dispuesto en el apartado 7.

Si un código de buenas prácticas no se ha podido finalizar a más tardar el 2 de agosto de 2025, o si la Oficina de IA lo considera inadecuado tras su evaluación con arreglo al apartado 6 del presente artículo, la Comisión podrá establecer, mediante actos de ejecución, normas comunes para el cumplimiento de las obligaciones establecidas en los artículos 53 y 55, que incluyan las cuestiones establecidas en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO VI

MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 57

Espacios controlados de pruebas para la IA

1. Los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional, que estará operativo a más tardar el 2 de agosto de 2026. Dicho espacio controlado de pruebas también podrá establecerse conjuntamente con las autoridades competentes de otros Estados miembros. La Comisión podrá proporcionar apoyo técnico, asesoramiento y herramientas para el establecimiento y el funcionamiento de los espacios controlados de pruebas para la IA.

La obligación prevista en el párrafo primero también podrá cumplirse mediante la participación en un espacio controlado de pruebas existente en la medida en que dicha participación proporcione un nivel de cobertura nacional equivalente a los Estados miembros participantes.

2. También podrán establecerse espacios controlados de pruebas para la IA adicionales a escala regional o local o conjuntamente con las autoridades competentes de otros Estados miembros.

3. El Supervisor Europeo de Protección de Datos también podrá establecer un espacio controlado de pruebas para la IA para las instituciones, órganos y organismos de la Unión, y podrá ejercer las funciones y tareas de las autoridades nacionales competentes de conformidad con el presente capítulo.

4. Los Estados miembros velarán por que las autoridades competentes a que se refieren los apartados 1 y 2 asignen recursos suficientes para cumplir lo dispuesto en el presente artículo de manera efectiva y oportuna. Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes del ecosistema de la IA. El presente artículo no afectará a otros espacios controlados de pruebas establecidos en virtud del Derecho de la Unión o nacional. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan esos otros espacios controlados de pruebas y las autoridades nacionales competentes.

5. Los espacios controlados de pruebas para la IA establecidos de conformidad con el apartado 1 proporcionarán un entorno controlado que fomente la innovación y facilite el desarrollo, el entrenamiento, 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, con arreglo a un plan del espacio controlado de pruebas específico acordado entre los proveedores o proveedores potenciales y la autoridad competente. Tales espacios controlados de pruebas podrán incluir pruebas en condiciones reales supervisadas dentro de ellos.

6. Las autoridades competentes proporcionarán, en su caso, orientación, supervisión y apoyo dentro del espacio controlado de pruebas para la IA con vistas a determinar los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, a las pruebas y a las medidas de reducción y su eficacia en relación con las obligaciones y los requisitos del presente Reglamento y, cuando proceda, de otras disposiciones de Derecho de la Unión y nacional cuya observancia se supervise en el espacio controlado de pruebas.

7. Las autoridades competentes proporcionarán a los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA orientaciones sobre las expectativas en materia de regulación y la manera de cumplir los requisitos y obligaciones establecidos en el presente Reglamento.

A petición del proveedor o proveedor potencial del sistema de IA, la autoridad competente aportará una prueba escrita de las actividades llevadas a cabo con éxito en el espacio controlado de pruebas. La autoridad competente también proporcionará un informe de salida en el que se detallen las actividades llevadas a cabo en el espacio controlado de pruebas y los resultados y resultados del aprendizaje correspondientes. Los proveedores podrán utilizar esta documentación para demostrar su cumplimiento del presente Reglamento mediante el proceso de evaluación de la conformidad o las actividades de vigilancia del mercado pertinentes. A este respecto, las autoridades de vigilancia del mercado y los organismos notificados tendrán en cuenta positivamente los informes de salida proporcionados y las pruebas escritas aportadas por la autoridad nacional competente, con vistas a acelerar los procedimientos de evaluación de la conformidad en una medida razonable.

8. Con sujeción a las disposiciones de confidencialidad del artículo 78 y con el acuerdo del proveedor o proveedor potencial, la Comisión y el Consejo de IA estarán autorizados a acceder a los informes de salida y los tendrán en cuenta, según proceda, en el ejercicio de sus funciones en virtud del presente Reglamento. Si tanto el proveedor o proveedor potencial como la autoridad nacional competente dan expresamente su acuerdo para ello, el informe de salida podrá hacerse público a través de la plataforma única de información a que se refiere el presente artículo.

9. El establecimiento de espacios controlados de pruebas para la IA tendrá por objeto contribuir a los siguientes objetivos:

a) mejorar la seguridad jurídica para lograr el cumplimiento del presente Reglamento o, en su caso, de otras disposiciones de Derecho de la Unión y nacional aplicable;

b) apoyar el intercambio de mejores prácticas mediante la cooperación con las autoridades que participan en el espacio controlado de pruebas para la IA;

c) fomentar la innovación y la competitividad y facilitar el desarrollo de un ecosistema de la IA;

d) contribuir a un aprendizaje normativo basado en datos contrastados;

e) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los proporcionen pymes, incluidas las empresas emergentes.

10. Las autoridades nacionales competentes 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 o competentes estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias.

11. Los espacios controlados de pruebas para la IA no afectarán a las facultades de supervisión o correctoras de las autoridades competentes que supervisan los espacios controlados de pruebas, tampoco a escala regional o local. Cualquier riesgo considerable para la salud, la seguridad y los derechos fundamentales detectado durante el proceso de desarrollo y prueba de estos sistemas de IA dará lugar a una reducción adecuada. Las autoridades nacionales competentes estarán facultadas para suspender temporal o permanentemente el proceso de prueba, o la participación en el espacio controlado de pruebas si no es posible una reducción efectiva, e informarán a la Oficina de IA de dicha decisión. Con el objetivo de apoyar la innovación en materia de IA en la Unión, las autoridades nacionales competentes ejercerán sus facultades de supervisión dentro de los límites del Derecho pertinente y harán uso de su potestad discrecional a la hora de aplicar disposiciones jurídicas en relación con un proyecto específico de espacio controlado de pruebas para la IA.

12. Los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA responderán, con arreglo al Derecho de la Unión y nacional en materia de responsabilidad, de cualquier daño infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas. Sin embargo, siempre que los proveedores potenciales respeten el plan específico y las condiciones de su participación y sigan de buena fe las orientaciones proporcionadas por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracciones del presente Reglamento. En los casos en que otras autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional hayan participado activamente en la supervisión del sistema de IA en el espacio controlado de pruebas y hayan proporcionado orientaciones para el cumplimiento, no se impondrán multas administrativas en relación con dichas disposiciones.

13. Los espacios controlados de pruebas para la IA serán diseñados y puestos en práctica de tal manera que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.

14. Las autoridades nacionales competentes coordinarán sus actividades y cooperarán en el marco del Consejo de IA.

15. Las autoridades nacionales competentes informarán a la Oficina de IA y al Consejo de IA del establecimiento de un espacio controlado de pruebas y podrán solicitarles apoyo y orientación. La Oficina de IA pondrá a disposición del público una lista de los espacios controlados de pruebas previstos y existentes y la mantendrá actualizada con el fin de fomentar una mayor interacción en los espacios controlados de pruebas para la IA, así como la cooperación transfronteriza.

16. Las autoridades nacionales competentes presentarán informes anuales a la Oficina de IA y al Consejo de IA, por primera vez un año después del establecimiento del espacio controlado de pruebas para la IA y, posteriormente, cada año hasta su terminación, así como un informe final. Dichos informes proporcionarán información sobre el progreso y los resultados de la puesta en práctica de dichos espacios controlados de pruebas, incluidos mejores prácticas, incidentes, enseñanzas extraídas y recomendaciones acerca de su configuración y, en su caso, acerca de la aplicación y posible revisión del presente Reglamento, incluidos sus actos delegados y de ejecución, y sobre la aplicación de otras disposiciones de Derecho de la Unión, supervisada por las autoridades competentes en el marco del espacio controlado de pruebas. Las autoridades nacionales competentes pondrán dichos informes anuales, o resúmenes de estos, a disposición del público, en línea. La Comisión tendrá en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones en virtud del presente Reglamento.

17. La Comisión desarrollará una interfaz única y específica que contenga toda la información pertinente relacionada con los espacios controlados de pruebas para la IA para que las partes interesadas puedan interactuar con los espacios controlados de pruebas para la IA y plantear consultas a las autoridades competentes, así como pedir orientaciones no vinculantes sobre la conformidad de productos, servicios y modelos de negocio innovadores que incorporen tecnologías de IA, de conformidad con el artículo 62, apartado 1, letra c). La Comisión se coordinará de forma proactiva con las autoridades nacionales competentes, cuando proceda.

Artículo 58

Disposiciones detalladas relativas a los espacios controlados de pruebas para la IA y al funcionamiento de dichos espacios

1. A fin de evitar que se produzca una fragmentación en la Unión, la Comisión adoptará actos de ejecución que especifiquen las disposiciones detalladas para el establecimiento, el desarrollo, la puesta en práctica, el funcionamiento y la supervisión de los espacios controlados de pruebas para la IA. Los actos de ejecución incluirán principios comunes sobre las siguientes cuestiones:

a) los criterios de admisibilidad y selección para participar en el espacio controlado de pruebas para la IA;

b) los procedimientos para la solicitud, la participación, la supervisión, la salida y la terminación del espacio controlado de pruebas para la IA, incluidos el plan del espacio controlado de pruebas y el informe de salida;

c) las condiciones aplicables a los participantes.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. Los actos de ejecución mencionados en el apartado 1 garantizarán:

a) que los espacios controlados de pruebas para la IA estén abiertos a cualquier proveedor o proveedor potencial de un sistema de IA que presente una solicitud y cumpla los criterios de admisibilidad y selección, que serán transparentes y equitativos, y también que las autoridades nacionales competentes informen a los solicitantes de su decisión en un plazo de tres meses a partir de la presentación de la solicitud;

b) que los espacios controlados de pruebas para la IA permitan un acceso amplio e igualitario y se adapten a la demanda de participación; los proveedores y proveedores potenciales también podrán presentar solicitudes en asociación con responsables del despliegue y con otros terceros pertinentes;

c) que las disposiciones detalladas y las condiciones relativas a los espacios controlados de pruebas para la IA propicien, en la medida de lo posible, que las autoridades nacionales competentes dispongan de flexibilidad para establecer y gestionar sus espacios controlados de pruebas para la IA;

d) que el acceso a los espacios controlados de pruebas para la IA sea gratuito para las pymes, incluidas las empresas emergentes, sin perjuicio de los costes excepcionales que las autoridades nacionales competentes puedan recuperar de una forma justa y proporcionada;

e) que se facilite a los proveedores y proveedores potenciales, mediante los resultados del aprendizaje de los espacios controlados de pruebas para la IA, el cumplimiento de las obligaciones de evaluación de la conformidad en virtud del presente Reglamento y la aplicación voluntaria de los códigos de conducta a que se refiere el artículo 95;

f) que los espacios controlados de pruebas para la IA faciliten la participación de otros agentes pertinentes del ecosistema de la IA, como los organismos notificados y los organismos de normalización, las pymes, incluidas las empresas emergentes, las empresas, los agentes innovadores, las instalaciones de ensayo y experimentación, los laboratorios de investigación y experimentación y los centros europeos de innovación digital, los centros de excelencia y los investigadores, a fin de permitir y facilitar la cooperación con los sectores público y privado;

g) que los procedimientos, procesos y requisitos administrativos para la solicitud, la selección, la participación y la salida del espacio controlado de pruebas para la IA sean sencillos y fácilmente inteligibles y se comuniquen claramente, a fin de facilitar la participación de las pymes, incluidas las empresas emergentes, con capacidades jurídicas y administrativas limitadas, y se racionalicen en toda la Unión, a fin de evitar la fragmentación y de que la participación en un espacio controlado de pruebas para la IA establecido por un Estado miembro o por el Supervisor Europeo de Protección de Datos esté reconocida mutua y uniformemente y tenga los mismos efectos jurídicos en toda la Unión;

h) que la participación en el espacio controlado de pruebas para la IA se limite a un período que se ajuste a la complejidad y la escala del proyecto, y que podrá ser prorrogado por la autoridad nacional competente;

i) que los espacios controlados de pruebas para la IA faciliten el desarrollo de herramientas e infraestructuras para la prueba, la evaluación comparativa, la evaluación y la explicación de las dimensiones de los sistemas de IA pertinentes para el aprendizaje normativo, como la precisión, la solidez y la ciberseguridad, así como de medidas para mitigar los riesgos para los derechos fundamentales y la sociedad en su conjunto.

3. Se ofrecerán a los proveedores potenciales que participen en los espacios controlados de pruebas para la IA, en particular a las pymes y las empresas emergentes, cuando proceda, servicios previos al despliegue, como orientaciones sobre la aplicación del presente Reglamento, otros servicios que aportan valor añadido, como ayuda con los documentos de normalización y la certificación, y acceso a las instalaciones de ensayo y experimentación, los centros europeos de innovación digital y los centros de excelencia.

4. Cuando las autoridades nacionales competentes estudien autorizar la realización de pruebas en condiciones reales supervisadas en el marco de un espacio controlado de pruebas para la IA que se establecerá en virtud del presente artículo, acordarán específicamente las condiciones de dichas pruebas y, en particular, las garantías adecuadas con los participantes, con vistas a proteger los derechos fundamentales, la salud y la seguridad. Cuando proceda, cooperarán con otras autoridades nacionales competentes con el fin de garantizar la coherencia de las prácticas en toda la Unión.

Artículo 59

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

1. En el espacio controlado de pruebas, los datos personales recabados lícitamente con otros fines podrán tratarse únicamente con el objetivo de desarrollar, entrenar y probar determinados sistemas de IA en el espacio controlado de pruebas cuando se cumplan todas las condiciones siguientes:

a) que los sistemas de IA se desarrollen para que una autoridad pública u otra persona física o jurídica proteja un interés público esencial en uno o varios de los siguientes ámbitos:

   i) la seguridad y la salud públicas, incluidos la detección, el diagnóstico, la prevención, el control y el tratamiento de enfermedades y la mejora de los sistemas sanitarios,

   ii) un elevado nivel de protección y mejora de la calidad del medio ambiente, la protección de la biodiversidad, la protección contra la contaminación, las medidas de transición ecológica, la mitigación del cambio climático y las medidas de adaptación a este,

   iii) la sostenibilidad energética,

   iv) la seguridad y la resiliencia de los sistemas de transporte y la movilidad, las infraestructuras críticas y las redes,

   v) la eficiencia y la calidad de la administración pública y de los servicios públicos;

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

c) que existan mecanismos de supervisión eficaces para detectar si pueden producirse durante la experimentación en el espacio controlado de pruebas riesgos elevados para los derechos y libertades de los interesados, mencionados en el artículo 35 del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725, así como mecanismos de respuesta para mitigar sin demora dichos riesgos y, en su caso, detener el tratamiento;

d) que 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 del proveedor potencial, y que únicamente las personas autorizadas tengan acceso a dichos datos;

e) que los proveedores solo puedan compartir los datos recabados originalmente de conformidad con el Derecho de la Unión en materia de protección de datos; los datos personales creados en el espacio controlado de pruebas no pueden salir del espacio controlado de pruebas;

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 ni afecte a la aplicación de sus derechos establecidos en el Derecho de la Unión en materia de protección de datos personales;

g) que los datos personales tratados en el contexto del espacio controlado de pruebas se protejan mediante medidas técnicas y organizativas adecuadas y 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, salvo que se disponga otra cosa en el Derecho de la Unión o el Derecho nacional;

i) que se conserve una descripción completa y detallada del proceso y la lógica subyacentes al 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; esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control fronterizo, de la inmigración o del asilo.

2. Cuando se lleve a cabo con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, y bajo el control y la responsabilidad de las autoridades garantes del cumplimiento del Derecho, el tratamiento de datos personales en los espacios controlados de pruebas para la IA se basará en un Derecho específico, de la Unión o nacional y cumplirá las condiciones acumulativas que se indican en el apartado 1.

3. El apartado 1 se entiende sin perjuicio del Derecho de la Unión o nacional que proscriba el tratamiento de datos personales con fines distintos de los expresamente mencionados en dichos actos, así como sin perjuicio del Derecho de la Unión o nacional que establezca las bases para el tratamiento de datos personales necesario para desarrollar, probar o entrenar sistemas innovadores de IA o de cualquier otra base jurídica, de conformidad con el Derecho de la Unión en materia de protección de datos personales.

Artículo 60

Pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA

1. Los proveedores o proveedores potenciales de sistemas de IA de alto riesgo enumerados en el anexo III podrán realizar pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA de conformidad el presente artículo y con el plan de la prueba en condiciones reales a que se refiere el presente artículo, sin perjuicio de las prohibiciones establecidas en el artículo 5.

La Comisión adoptará, mediante un acto de ejecución, los elementos detallados del plan de la prueba en condiciones reales. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

El presente apartado se entiende sin perjuicio del Derecho de la Unión o nacional en materia de pruebas en condiciones reales de sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I.

2. Los proveedores o proveedores potenciales podrán realizar pruebas de los sistemas de IA de alto riesgo mencionados en el anexo III en condiciones reales en cualquier momento antes de la introducción en el mercado o la puesta en servicio del sistema de IA por cuenta propia o en asociación con uno o varios responsables del despliegue o responsables del despliegue potenciales.

3. Las pruebas de sistemas de IA de alto riesgo en condiciones reales con arreglo al presente artículo se entenderán sin perjuicio de cualquier revisión ética que se exija en el Derecho de la Unión o nacional.

4. Los proveedores o proveedores potenciales podrán realizar pruebas en condiciones reales solamente cuando se cumplan todas las condiciones siguientes:

a) el proveedor o proveedor potencial ha elaborado un plan de la prueba en condiciones reales y lo ha presentado a la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales;

b) la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales ha aprobado las pruebas en condiciones reales y el plan de la prueba en condiciones reales; si la autoridad de vigilancia del mercado no responde en un plazo de treinta días, se entenderá que las pruebas en condiciones reales y el plan de la prueba en condiciones reales han sido aprobados; cuando el Derecho nacional no contemple una aprobación tácita, las pruebas en condiciones reales estarán sujetas a una autorización también en este caso;

c) el proveedor o proveedor potencial, con excepción de los proveedores o proveedores potenciales de sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, así como de los sistemas de IA de alto riesgo mencionados en el punto 2 del anexo III ha registrado las pruebas en condiciones reales de conformidad con el artículo 71, apartado 4, con un número de identificación único para toda la Unión y la información indicada en el anexo IX; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, ha registrado las pruebas en condiciones reales en la parte no pública de la base de datos de la UE de conformidad con el artículo 49, apartado 4, letra d), con un número de identificación único para toda la Unión y la información indicada en este; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, ha registrado las pruebas en condiciones reales de conformidad con el artículo 49, apartado 5;

d) el proveedor o proveedor potencial que realiza las pruebas en condiciones reales está establecido en la Unión o ha designado a un representante legal que está establecido en la Unión;

e) los datos recabados y tratados a efectos de las pruebas en condiciones reales únicamente se transferirán a terceros países si se aplican las garantías adecuadas y aplicables en virtud del Derecho de la Unión;

f) las pruebas en condiciones reales no duran más de lo necesario para lograr sus objetivos y, en cualquier caso, no más de seis meses, que podrán prorrogarse por un período adicional de seis meses, con sujeción al envío de una notificación previa por parte del proveedor o proveedor potencial a la autoridad de vigilancia del mercado, acompañada por una explicación de la necesidad de dicha prórroga;

g) los sujetos de las pruebas en condiciones reales que sean personas pertenecientes a colectivos vulnerables debido a su edad o a una discapacidad cuentan con protección adecuada;

h) cuando un proveedor o proveedor potencial organice las pruebas en condiciones reales en cooperación con uno o varios responsables del despliegue o responsables del despliegue potenciales, estos últimos habrán sido informados de todos los aspectos de las pruebas que resulten pertinentes para su decisión de participar y habrán recibido las instrucciones de uso pertinentes del sistema de IA a que se refiere el artículo 13; el proveedor o proveedor potencial y el responsable del despliegue o responsable del despliegue potencial alcanzarán un acuerdo en que se detallen sus funciones y responsabilidades con vistas a garantizar el cumplimiento de las disposiciones relativas a las pruebas en condiciones reales con arreglo al presente Reglamento y a otras disposiciones de Derecho de la Unión y nacional aplicable;

i) los sujetos de las pruebas en condiciones reales han dado su consentimiento informado de conformidad con el artículo 61 o, en el ámbito de la garantía del cumplimiento del Derecho, en el que intentar obtener el consentimiento informado impediría que se probara el sistema de IA, las pruebas en sí y los resultados de las pruebas en condiciones reales no tendrán ningún efecto negativo sobre los sujetos, cuyos datos personales se suprimirán una vez realizada la prueba;

j) las pruebas en condiciones reales son supervisadas de manera efectiva por el proveedor o el proveedor potencial y por los responsables del despliegue o los responsables del despliegue potenciales mediante personas adecuadamente cualificadas en el ámbito pertinente y con la capacidad, formación y autoridad necesarias para realizar sus tareas;

k) se pueden revertir y descartar de manera efectiva las predicciones, recomendaciones o decisiones del sistema de IA.

5. Cualquier sujeto de las pruebas en condiciones reales o su representante legalmente designado, según proceda, podrá, sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación, abandonar las pruebas en cualquier momento retirando su consentimiento informado y solicitar la supresión inmediata y permanente de sus datos personales. La retirada del consentimiento informado no afectará a las actividades ya completadas.

6. De conformidad con el artículo 75, los Estados miembros conferirán a sus autoridades de vigilancia del mercado poderes para exigir a los proveedores y proveedores potenciales que faciliten información, realizar sin previo aviso inspecciones a distancia o *in situ* y controlar la realización de las pruebas en condiciones reales y los sistemas de IA de alto riesgo relacionados. Las autoridades de vigilancia del mercado harán uso de dichos poderes para garantizar que las pruebas en condiciones reales se desarrollen de manera segura.

7. Se informará de cualquier incidente grave detectado en el transcurso de las pruebas en condiciones reales a la autoridad nacional de vigilancia del mercado de conformidad con el artículo 73. El proveedor o proveedor potencial adoptará medidas de reducción inmediatas o, en su defecto, suspenderá las pruebas en condiciones reales hasta que se produzca dicha reducción o pondrá fin a las pruebas. El proveedor o proveedor potencial establecerá un procedimiento para la rápida recuperación del sistema de IA en caso de que se ponga fin a las pruebas en condiciones reales.

8. El proveedor o proveedor potencial notificará a la autoridad nacional de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales la suspensión o la terminación de las pruebas en condiciones reales y los resultados finales.

9. El proveedor o proveedor potencial será responsable, conforme al Derecho de la Unión y nacional en materia de responsabilidad aplicable, de cualquier daño causado en el transcurso de sus pruebas en condiciones reales.

Artículo 61

Consentimiento informado para participar en pruebas en condiciones reales fuera de los espacios controlados de pruebas para la IA

1. A los efectos de las pruebas en condiciones reales con arreglo al artículo 60, se obtendrá de los sujetos de las pruebas un consentimiento informado dado libremente antes de participar en dichas pruebas y después de haber recibido información concisa, clara, pertinente y comprensible en relación con:

a) la naturaleza y los objetivos de las pruebas en condiciones reales y los posibles inconvenientes asociados a su participación;

b) las condiciones en las que se van a llevar a cabo las pruebas en condiciones reales, incluida la duración prevista de la participación del sujeto o los sujetos;

c) sus derechos y las garantías relativas a su participación, en particular su derecho a negarse a participar y el derecho a abandonar las pruebas en condiciones reales en cualquier momento sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación;

d) las disposiciones para solicitar la reversión o el descarte de las predicciones, recomendaciones o decisiones del sistema de IA;

e) el número de identificación único para toda la Unión de la prueba en condiciones reales de conformidad con el artículo 60, apartado 4, letra c), y la información de contacto del proveedor o de su representante legal, de quien se puede obtener más información.

2. El consentimiento informado estará fechado y documentado, y se entregará una copia a los sujetos de la prueba o a sus representantes legales.

Artículo 62

Medidas dirigidas a proveedores y responsables del despliegue, en particular pymes, incluidas las empresas emergentes

1. Los Estados miembros adoptarán las medidas siguientes:

a) proporcionarán a las pymes, incluidas las empresas emergentes, que tengan un domicilio social o una sucursal en la Unión un acceso prioritario a los espacios controlados de pruebas para la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección; el acceso prioritario no impedirá que otras pymes, incluidas las empresas emergentes, distintas de las mencionadas en el presente apartado accedan al espacio controlado de pruebas para la IA, siempre que también cumplan las condiciones de admisibilidad y los criterios de selección;

b) organizarán actividades de sensibilización y formación específicas sobre la aplicación del presente Reglamento adaptadas a las necesidades de las pymes, incluidas las empresas emergentes, los responsables del despliegue y, en su caso, las autoridades públicas locales;

c) utilizarán canales específicos existentes y establecerán, en su caso, nuevos canales para la comunicación con las pymes, incluidas las empresas emergentes, los responsables del despliegue y otros agentes innovadores, así como, en su caso, las autoridades públicas locales, a fin de proporcionar asesoramiento y responder a las dudas planteadas acerca de la aplicación del presente Reglamento, también en relación con la participación en los espacios controlados de pruebas para la IA;

d) fomentarán la participación de las pymes y otras partes interesadas pertinentes en el proceso de desarrollo de la normalización.

2. Se tendrán en cuenta los intereses y necesidades específicos de los proveedores que sean pymes, incluidas las empresas emergentes, a la hora de fijar las tasas para la evaluación de la conformidad en virtud del artículo 43, y se reducirán dichas tasas en proporción a su tamaño, al tamaño del mercado y a otros indicadores pertinentes.

3. La Oficina de IA adoptará las medidas siguientes:

a) proporcionará modelos normalizados para los ámbitos regulados por el presente Reglamento, tal como especifique el Consejo de IA en su solicitud;

b) desarrollará y mantendrá una plataforma única de información que proporcione información fácil de usar en relación con el presente Reglamento destinada a todos los operadores de la Unión;

c) organizará campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento;

d) evaluará y fomentará la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

Artículo 63

Excepciones para operadores específicos

1. Las microempresas en el sentido de la Recomendación 2003/361/CE podrán cumplir determinados elementos del sistema de gestión de la calidad exigido por el artículo 17 del presente Reglamento de manera simplificada, siempre que no tengan empresas asociadas o empresas vinculadas en el sentido de dicha Recomendación. A tal fin, la Comisión elaborará directrices sobre los elementos del sistema de gestión de la calidad que puedan cumplirse de manera simplificada teniendo en cuenta las necesidades de las microempresas sin que ello afecte al nivel de protección ni a la necesidad de cumplir los requisitos relativos a los sistemas de IA de alto riesgo.

2. El apartado 1 del presente artículo no se interpretará en el sentido de que exime a dichos operadores de cumplir cualquier otro requisito u obligación establecidos en el presente Reglamento, incluidos aquellos que figuran en los artículos 9, 10, 11, 12, 13, 14, 15, 72 y 73.

CAPÍTULO VII

GOBERNANZA

SECCIÓN 1

Gobernanza a escala de la Unión

Artículo 64

Oficina de IA

1. La Comisión desarrollará los conocimientos especializados y las capacidades de la Unión en el ámbito de la IA mediante la Oficina de IA.

2. Los Estados miembros facilitarán las tareas encomendadas a la Oficina de IA, que están reflejadas en el presente Reglamento.

Artículo 65

Creación y estructura del Consejo Europeo de Inteligencia Artificial

1. Se crea un Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»).

2. El Consejo de IA estará compuesto de un representante por Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Oficina de IA también asistirá a las reuniones del Consejo de IA sin participar en las votaciones. El Consejo de IA podrá invitar a otras autoridades, organismos o expertos nacionales y de la Unión a las reuniones en función de cada situación concreta, cuando los temas tratados sean relevantes para ellos.

3. Cada representante será designado por su Estado miembro por un período de tres años, renovable una vez.

4. Los Estados miembros se asegurarán de que sus representantes en el Consejo de IA:

a) tengan las competencias y los poderes pertinentes en su Estado miembro para poder contribuir activamente al cumplimiento de las funciones del Consejo de IA a que se refiere el artículo 66;

b) sean designados como punto de contacto único respecto del Consejo de IA y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;

c) estén facultados para facilitar la coherencia y la coordinación entre las autoridades nacionales competentes en su Estado miembro en relación con la aplicación del presente Reglamento, también mediante la recopilación de datos e información pertinentes para cumplir sus funciones en el Consejo de IA.

5. Los representantes designados de los Estados miembros adoptarán el Reglamento Interno del Consejo de IA por mayoría de dos tercios. El Reglamento Interno establecerá, en particular, los procedimientos para el proceso de selección, la duración del mandato y las especificaciones de las funciones de la presidencia, las modalidades de votación detalladas y la organización de las actividades del Consejo de IA y de sus subgrupos.

6. El Consejo de IA establecerá dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y de notificar a las autoridades cuestiones relacionadas con la vigilancia del mercado y los organismos notificados, respectivamente.

El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020.

El Consejo de IA puede establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. Cuando proceda, se podrá invitar a representantes del foro consultivo a que se refiere el artículo 67 a dichos subgrupos o a reuniones específicas de dichos subgrupos en calidad de observadores.

7. El Consejo de IA se organizará y gestionará de manera que se preserve la objetividad e imparcialidad de sus actividades.

8. El Consejo de IA estará presidido por uno de los representantes de los Estados miembros. La Oficina de IA asumirá las labores de secretaría del Consejo de IA, convocará las reuniones a petición de la presidencia y elaborará el orden del día de conformidad con las funciones del Consejo de IA en virtud del presente Reglamento y de su Reglamento Interno.

Artículo 66

Funciones del Consejo de IA

El Consejo de IA prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del presente Reglamento. A tal fin, el Consejo de IA podrá, en particular:

a) contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del presente Reglamento y, en cooperación con las autoridades de vigilancia del mercado de que se trate y previo acuerdo de estas, apoyar las actividades conjuntas de las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartado 11;

b) recopilar y compartir conocimientos técnicos y reglamentarios y mejores prácticas entre los Estados miembros;

c) ofrecer asesoramiento sobre la aplicación del presente Reglamento, en particular en lo relativo al cumplimiento de las normas sobre modelos de IA de uso general;

d) contribuir a la armonización de las prácticas administrativas en los Estados miembros, también en relación con la exención de los procedimientos de evaluación de la conformidad a que se refiere el artículo 46, el funcionamiento de los espacios controlados de pruebas para la IA y las pruebas en condiciones reales a que se refieren los artículos 57, 59 y 60;

e) previa solicitud de la Comisión o por iniciativa propia, emitir recomendaciones y dictámenes por escrito en relación con cualquier asunto pertinente relacionado con la ejecución del presente Reglamento y con su aplicación coherente y eficaz, por ejemplo:

   i) sobre la elaboración y aplicación de códigos de conducta y códigos de buenas prácticas con arreglo al presente Reglamento, así como de las directrices de la Comisión,

   ii) sobre la evaluación y revisión del presente Reglamento con arreglo al artículo 112, también en lo que respecta a los informes de incidentes graves a que se refiere el artículo 73, y el funcionamiento de la base de datos de la UE a que se refiere el artículo 71, la preparación de los actos delegados o de ejecución, y en lo que respecta a las posibles adaptaciones del presente Reglamento a los actos legislativos de armonización de la Unión enumerados en el anexo I,

   iii) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el capítulo III, sección 2,

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

v) sobre tendencias, como la competitividad de Europa a escala mundial en materia de IA, la adopción de la IA en la Unión y el desarrollo de capacidades digitales,

vi) sobre tendencias en la tipología cambiante de las cadenas de valor de la IA, en particular sobre las implicaciones resultantes en términos de rendición de cuentas,

vii) sobre la posible necesidad de modificar el anexo III de conformidad con el artículo 7 y sobre la posible necesidad de revisar el artículo 5 con arreglo al artículo 112, teniendo en cuenta las pruebas disponibles pertinentes y los últimos avances tecnológicos;

f) apoyar a la Comisión en la promoción de la alfabetización en materia de IA, la sensibilización del público y la comprensión de las ventajas, los riesgos, las salvaguardias y los derechos y obligaciones en relación con la utilización de sistemas de IA;

g) facilitar el desarrollo de criterios comunes y la comprensión compartida entre los operadores del mercado y las autoridades competentes de los conceptos pertinentes previstos en el presente Reglamento, por ejemplo, contribuyendo al desarrollo de parámetros de referencia;

h) cooperar, en su caso, con otras instituciones, órganos y organismos de la Unión, así como con grupos de expertos y redes pertinentes de la Unión, en particular en los ámbitos de la seguridad de los productos, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, la protección de los consumidores, y la protección de datos y de los derechos fundamentales;

i) contribuir a la cooperación efectiva con las autoridades competentes de terceros países y con organizaciones internacionales;

j) asistir a las autoridades nacionales competentes y a la Comisión en el desarrollo de los conocimientos técnicos y organizativos necesarios para la aplicación del presente Reglamento, por ejemplo, contribuyendo a la evaluación de las necesidades de formación del personal de los Estados miembros que participe en dicha aplicación;

k) asistir a la Oficina de IA en el apoyo a las autoridades nacionales competentes para el establecimiento y el desarrollo de espacios controlados de pruebas para la IA, y facilitar la cooperación y el intercambio de información entre espacios controlados de pruebas para la IA;

l) contribuir a la elaboración de documentos de orientación y proporcionar el asesoramiento pertinente al respecto;

m) proporcionar asesoramiento a la Comisión en relación con asuntos internacionales en materia de IA;

n) emitir dictámenes para la Comisión sobre las alertas cualificadas relativas a modelos de IA de uso general;

o) recibir dictámenes de los Estados miembros sobre alertas cualificadas relativas a modelos de IA de uso general y sobre las experiencias y prácticas nacionales en materia de supervisión y ejecución de los sistemas de IA, en particular los sistemas que integran los modelos de IA de uso general.

Artículo 67

Foro consultivo

1. Se creará un foro consultivo para proporcionar conocimientos técnicos y asesorar al Consejo de IA y a la Comisión, así como para contribuir a las funciones de estos en virtud del presente Reglamento.

2. La composición del foro consultivo representará una selección equilibrada de partes interesadas, incluidos la industria, las empresas emergentes, las pymes, la sociedad civil y el mundo académico. La composición del foro consultivo estará equilibrada en lo que respecta a los intereses comerciales y los no comerciales y, dentro de la categoría de los intereses comerciales, en lo que respecta a las pymes y otras empresas.

3. La Comisión nombrará a los miembros del foro consultivo, de conformidad con los criterios establecidos en el apartado 2, de entre las partes interesadas con conocimientos especializados reconocidos en el ámbito de la IA.

4. El mandato de los miembros del foro consultivo será de dos años y podrá prorrogarse hasta un máximo de cuatro años.

5. La Agencia de los Derechos Fundamentales de la Unión Europea, la Agencia de la Unión Europea para la Ciberseguridad, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) serán miembros permanentes del foro consultivo.

6. El foro consultivo establecerá su reglamento interno. Elegirá dos copresidentes de entre sus miembros, de conformidad con los criterios establecidos en el apartado 2. El mandato de los copresidentes será de dos años, renovable una sola vez.

7. El foro consultivo celebrará reuniones al menos dos veces al año. Podrá invitar a expertos y otras partes interesadas a sus reuniones.

8. El foro consultivo podrá elaborar dictámenes, recomendaciones y contribuciones por escrito a petición del Consejo de IA o de la Comisión.

9. El foro consultivo podrá crear subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento.

10. El foro consultivo redactará un informe anual de sus actividades. Dicho informe se pondrá a disposición del público.

Artículo 68

Grupo de expertos científicos independientes

1. La Comisión adoptará, mediante un acto de ejecución, disposiciones sobre la creación de un grupo de expertos científicos independientes (en lo sucesivo, «grupo de expertos científicos») destinado a apoyar las actividades de garantía del cumplimiento previstas en el presente Reglamento. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. El grupo de expertos científicos estará compuesto por expertos seleccionados por la Comisión sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA necesarios para las funciones establecidas en el apartado 3, y será capaz de demostrar que cumple todas las condiciones siguientes:

a) conocimientos especializados y competencias particulares, y conocimientos científicos o técnicos en el ámbito de la IA;

b) independencia de cualquier proveedor de sistemas de IA o de modelos de IA de uso general;

c) capacidad para llevar a cabo actividades con diligencia, precisión y objetividad.

La Comisión, en consulta con el Consejo de IA, determinará el número de expertos del grupo de acuerdo con las necesidades requeridas y garantizará una representación geográfica y de género justa.

3. El grupo de expertos científicos asesorará y apoyará a la Oficina de IA, en particular en lo que respecta a las siguientes funciones:

a) apoyar la aplicación y el cumplimiento del presente Reglamento en lo que respecta a los sistemas y modelos de IA de uso general, en particular:

   i) alertando a la Oficina de IA de los posibles riesgos sistémicos a escala de la Unión de modelos de IA de uso general, de conformidad con el artículo 90,

   ii) contribuyendo al desarrollo de herramientas y metodologías para evaluar las capacidades de los sistemas y modelos de IA de uso general, también a través de parámetros de referencia,

   iii) asesorando sobre la clasificación de modelos de IA de uso general con riesgo sistémico,

   iv) asesorando sobre la clasificación de diversos sistemas y modelos de IA de uso general,

v) contribuyendo al desarrollo de herramientas y modelos;

b) apoyar la labor de las autoridades de vigilancia del mercado, a petición de estas;

c) apoyar las actividades transfronterizas de vigilancia del mercado a que se refiere el artículo 74, apartado 11, sin perjuicio de los poderes de las autoridades de vigilancia del mercado;

d) apoyar a la Oficina de IA en el ejercicio de sus funciones en el contexto del procedimiento de salvaguardia de la Unión con arreglo al artículo 81.

4. Los expertos del grupo desempeñarán sus funciones con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades. No solicitarán ni aceptarán instrucciones de nadie en el ejercicio de sus funciones previstas en el apartado 3. Cada experto cumplimentará una declaración de intereses que se hará pública. La Oficina de IA establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.

5. El acto de ejecución a que se refiere el apartado 1 incluirá disposiciones sobre las condiciones, los procedimientos y las disposiciones detalladas para que el grupo de expertos científicos y sus miembros emitan alertas y soliciten la asistencia de la Oficina de IA para el desempeño de las funciones del grupo de expertos científicos.

Artículo 69

Acceso a expertos por parte de los Estados miembros

1. Los Estados miembros podrán recurrir a expertos del grupo de expertos científicos para que apoyen sus actividades de garantía del cumplimiento previstas en el presente Reglamento.

2. Se podrá exigir a los Estados miembros que paguen tasas por el asesoramiento y el apoyo prestado por los expertos. La estructura y el importe de las tasas, así como la escala y la estructura de los costes recuperables, se establecerán en el acto de ejecución a que se refiere el artículo 68, apartado 1, teniendo en cuenta los objetivos de la correcta aplicación del presente Reglamento, la rentabilidad y la necesidad de garantizar que todos los Estados miembros tengan un acceso efectivo a los expertos.

3. La Comisión facilitará el acceso oportuno de los Estados miembros a los expertos, según sea necesario, y garantizará que la combinación de las actividades de apoyo llevadas a cabo por las estructuras de apoyo a los ensayos de IA de la Unión con arreglo al artículo 84 y por expertos con arreglo al presente artículo se organice de manera eficiente y ofrezca el mayor valor añadido posible.

SECCIÓN 2

Autoridades nacionales competentes

Artículo 70

Designación de las autoridades nacionales competentes y de los puntos de contacto único

1. Cada Estado miembro establecerá o designará al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes a los efectos del presente Reglamento. Dichas autoridades nacionales competentes ejercerán sus poderes de manera independiente, imparcial y sin sesgos, a fin de preservar la objetividad de sus actividades y funciones y de garantizar la aplicación y ejecución del presente Reglamento. Los miembros de dichas autoridades se abstendrán de todo acto incompatible con sus funciones. Siempre que se respeten esos principios, tales actividades y funciones podrán ser realizadas por una o varias autoridades designadas, de conformidad con las necesidades organizativas del Estado miembro.

2. Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. Los Estados miembros pondrán a disposición del público, por medios de comunicación electrónica, información sobre la forma de contactar con las autoridades competentes y los puntos de contacto únicos a más tardar el 2 de agosto de 2025. Los Estados miembros designarán una autoridad de vigilancia del mercado que actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad de dicho punto. La Comisión pondrá a disposición del público la lista de puntos de contacto únicos.

3. Los Estados miembros garantizarán que sus autoridades nacionales competentes dispongan de recursos técnicos, financieros y humanos adecuados, y de infraestructuras para el desempeño de sus funciones de manera efectiva 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 IA, datos y computación de datos; la protección de los datos personales, la ciberseguridad, los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes. Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.

4. Las autoridades nacionales competentes adoptarán las medidas adecuadas para garantizar un nivel adecuado de ciberseguridad.

5. En el desempeño de sus funciones, las autoridades nacionales competentes actuarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

6. A más tardar el 2 de agosto de 2025 y cada dos años a partir de entonces, los Estados miembros presentarán a la Comisión un informe acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión remitirá dicha información al Consejo de IA para que mantenga un debate sobre ella y, en su caso, formule recomendaciones.

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

8. Las autoridades nacionales competentes podrán proporcionar orientaciones y asesoramiento sobre la aplicación del presente Reglamento, en particular a las pymes —incluidas las empresas emergentes—, teniendo en cuenta las orientaciones y el asesoramiento del Consejo de IA y de la Comisión, según proceda. Siempre que una autoridad nacional competente tenga la intención de proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otros actos del Derecho de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dichos actos, según proceda.

9. Cuando las instituciones, órganos 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.

CAPÍTULO VIII

BASE DE DATOS DE LA UE PARA SISTEMAS DE IA DE ALTO RIESGO

Artículo 71

Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el ANEXO III

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contendrá la información mencionada en los apartados 2 y 3 del presente artículo en relación con los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, que estén registrados con arreglo a los artículos 49 y 60 y los sistemas de IA que no se consideren de alto riesgo en virtud del artículo 6, apartado 3, y que estén registrados con arreglo al artículo 6, apartado 4, y al artículo 49. La Comisión consultará a los expertos pertinentes a la hora de fijar las especificaciones funcionales de dicha base de datos y al Consejo de IA a la hora de actualizarlas.

2. Los datos enumerados en el anexo VIII, secciones A y B, serán introducidos en la base de datos de la UE por el proveedor o, en su caso, por el representante autorizado.

3. Los datos enumerados en el anexo VIII, sección C, serán introducidos en la base de datos de la UE por el responsable del despliegue que sea una autoridad pública, órgano u organismo, o actúe en su nombre, de conformidad con el artículo 49, apartados 3 y 4.

4. A excepción de la sección a que se refieren el artículo 49, apartado 4, y el artículo 60, apartado 4, letra c), la información presente en la base de datos de la UE y registrada de conformidad con lo dispuesto en el artículo 49 será accesible y estará a disposición del público de manera sencilla. Debe ser fácil navegar por la información y esta ha de ser legible por máquina. Únicamente podrán acceder a la información registrada de conformidad con el artículo 60 las autoridades de vigilancia de mercado y la Comisión, a menos que el proveedor potencial o el proveedor hayan dado su consentimiento a que la información también esté accesible para el público.

5. La base de datos de la UE únicamente contendrá datos personales en la medida en 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 o al responsable del despliegue, según proceda.

6. La Comisión será la responsable del tratamiento de la base de datos de la UE, y proporcionará apoyo técnico y administrativo adecuado a los proveedores, proveedores potenciales y responsables del despliegue. La base de datos de la UE cumplirá los requisitos de accesibilidad aplicables.

CAPÍTULO IX

VIGILANCIA POSCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN Y VIGILANCIA DEL MERCADO

SECCIÓN 1

Vigilancia poscomercialización

Artículo 72

Vigilancia poscomercialización por parte de los proveedores y plan de vigilancia poscomercialización para sistemas de IA de alto riesgo

1. Los proveedores establecerán y documentarán un sistema de vigilancia poscomercialización de forma proporcionada a la naturaleza de las tecnologías de IA y a los riesgos de los sistemas de IA de alto riesgo.

2. El sistema de vigilancia poscomercialización recopilará, documentará y analizará de manera activa y sistemática los datos pertinentes que pueden facilitar los responsables del despliegue o que pueden recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y que permiten al proveedor evaluar el cumplimiento permanente de los requisitos establecidos en el capítulo III, sección 2, por parte de los sistemas de IA. Cuando proceda, la vigilancia poscomercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue que sean autoridades garantes del cumplimiento del Derecho.

3. El sistema de vigilancia poscomercialización se basará en un plan de vigilancia poscomercialización. El plan de vigilancia poscomercialización 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 vigilancia poscomercialización y la lista de elementos que deberán incluirse en él a más tardar el 2 de febrero de 2026. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

4. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando ya se hayan establecido un sistema y un plan de vigilancia poscomercialización con arreglo a dichos actos, con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los elementos necesarios descritos en los apartados 1, 2 y 3, utilizando el modelo a que se refiere el apartado 3, en los sistemas y planes que ya existan en virtud de dicha legislación, siempre que alcance un nivel de protección equivalente.

El párrafo primero del presente apartado también se aplicará a los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, introducidos en el mercado o puestos en servicio por entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros.

SECCIÓN 2

Intercambio de información sobre incidentes graves

Artículo 73

Notificación de incidentes graves

1. Los proveedores de sistemas de IA de alto riesgo introducidos en el mercado de la Unión notificarán cualquier incidente grave a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya producido dicho incidente.

2. La notificación a que se refiere el apartado 1 se efectuará inmediatamente después de que el proveedor haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista dicho vínculo y, en cualquier caso, a más tardar quince días después de que el proveedor o, en su caso, el responsable del despliegue, tengan conocimiento del incidente grave.

El plazo para la notificación a que se refiere el párrafo primero tendrá en cuenta la magnitud del incidente grave.

3. No obstante lo dispuesto en el apartado 2 del presente artículo, en caso de una infracción generalizada o de un incidente grave tal como se define en el artículo 3, punto 49, letra b), la notificación a que se refiere el apartado 1 del presente artículo se realizará de manera inmediata y a más tardar dos días después de que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente.

4. No obstante lo dispuesto en el apartado 2, en caso de fallecimiento de una persona, la notificación se efectuará de manera inmediata después de que el proveedor o el responsable del despliegue haya establecido —o tan pronto como sospeche— una relación causal entre el sistema de IA de alto riesgo y el incidente grave, en un plazo no superior a diez días a contar de la fecha en la que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente grave.

5. Cuando sea necesario para garantizar la notificación en tiempo oportuno, el proveedor o, en su caso, el responsable del despliegue podrá presentar inicialmente una notificación incompleta, seguida de una notificación completa.

6. Después de notificar un incidente grave con arreglo al apartado 1, el proveedor realizará sin demora las investigaciones necesarias en relación con el incidente grave y el sistema de IA afectado. Esto incluirá una evaluación de riesgos del incidente y las medidas correctoras.

El proveedor cooperará con las autoridades competentes y, en su caso, con el organismo notificado afectado durante las investigaciones a que se refiere el párrafo primero, y no emprenderá acción alguna que suponga la modificación del sistema de IA afectado de un modo que pueda repercutir en cualquier evaluación posterior de las causas del incidente sin haber informado antes de dicha acción a las autoridades competentes.

7. Tras la recepción de una notificación relativa a un incidente grave a que se refiere el artículo 3, punto 49, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el 2 de agosto de 2025 y se evaluarán periódicamente.

8. La autoridad de vigilancia del mercado adoptará medidas adecuadas tal como se establece en el artículo 19 del Reglamento (UE) 2019/1020, en un plazo de siete días a partir de la fecha en que reciba la notificación a que se refiere el apartado 1 del presente artículo, y seguirá los procedimientos de notificación previstos en dicho Reglamento.

9. En el caso de los sistemas de IA de alto riesgo a que se refiere el anexo III, introducidos en el mercado o puestos en servicio por proveedores que estén sujetos a instrumentos legislativos de la Unión por los que se establezcan obligaciones de información equivalentes a las establecidas en el presente Reglamento, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c).

10. 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 los Reglamento (UE) 2017/745 y (UE) 2017/746, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c), del presente Reglamento, y se hará a la autoridad nacional competente elegida para tal fin por los Estados miembros en los que se haya producido el incidente.

11. Las autoridades nacionales competentes informarán de inmediato a la Comisión de todo incidente grave, independientemente de han adoptado medidas al respecto, de conformidad con el artículo 20 del Reglamento (UE) 2019/1020.

SECCIÓN 3

Garantía del cumplimiento

Artículo 74

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 regulados por el presente Reglamento. A efectos de garantía del cumplimiento efectivo 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 mencionados en el artículo 2, apartado 1, 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. Como parte de sus obligaciones de presentación de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado informarán anualmente a la Comisión y a las autoridades nacionales de competencia pertinentes de 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. Asimismo, informarán anualmente a la Comisión sobre el recurso a prácticas prohibidas que se hayan producido durante ese año y sobre las medidas adoptadas.

3. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designada en virtud de dichos actos legislativos.

Como excepción a lo dispuesto en el párrafo primero, en circunstancias adecuadas, los Estados miembros podrán designar otra autoridad pertinente como autoridad de vigilancia del mercado, siempre que se garantice la coordinación con las autoridades sectoriales de vigilancia del mercado pertinentes responsables de la ejecución de los actos legislativos de armonización de la Unión enumerados en el anexo I.

4. Los procedimientos a que se refieren los artículos 79 a 83 del presente Reglamento no se aplicarán a los sistemas de IA asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando dichos actos legislativos ya prevean procedimientos que garanticen un nivel equivalente de protección que tengan el mismo objetivo. En dichos casos, se aplicarán los procedimientos sectoriales pertinentes.

5. Sin perjuicio de los poderes de las autoridades de vigilancia del mercado en virtud del artículo 14 del Reglamento (UE) 2019/1020, a efectos de garantizar la ejecución efectiva del presente Reglamento, las autoridades de vigilancia del mercado podrán ejercer a distancia los poderes a que se refiere el artículo 14, apartado 4, letras d) y j), de dicho Reglamento, según proceda.

6. En el caso de los sistemas de IA de alto riesgo introducidos en el mercado, puestos en servicio o utilizados por entidades financieras reguladas por el Derecho de la Unión en materia de servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad nacional pertinente responsable de la supervisión financiera de dichas entidades con arreglo a la mencionada legislación, en la medida en que la introducción en el mercado, la puesta en servicio o la utilización del sistema de IA esté directamente relacionada con la prestación de dichos servicios financieros.

7. Como excepción a lo dispuesto en el apartado 6, en las circunstancias apropiadas y siempre que se garantice la coordinación, el Estado miembro podrá designar otra autoridad pertinente como autoridad de vigilancia del mercado a efectos del presente Reglamento.

Las autoridades nacionales de vigilancia del mercado que supervisen las entidades de crédito reguladas por la Directiva 2013/36/UE y que participen en el Mecanismo Único de Supervisión establecido por el Reglamento (UE) n.º 1024/2013 deberán comunicar sin demora al Banco Central Europeo toda información obtenida en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

8. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1, en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento, 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 competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades en el ejercicio de su función judicial.

9. Cuando las instituciones, órganos y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como su autoridad de vigilancia del mercado, salvo en relación con el Tribunal de Justicia de la Unión Europea cuando actúe en el ejercicio de su función judicial.

10. 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 indicada en el anexo I o en otras disposiciones de Derecho de la Unión que pudieran resultar pertinente para los sistemas de IA de alto riesgo a que se refiere el anexo III.

11. Las autoridades de vigilancia del mercado y la Comisión podrán proponer actividades conjuntas, incluidas investigaciones conjuntas, que deben llevar a cabo bien las autoridades de vigilancia del mercado, bien las autoridades de vigilancia del mercado junto con la Comisión, con el objetivo de fomentar el cumplimiento, detectar incumplimientos, sensibilizar u ofrecer orientaciones en relación con el presente Reglamento con respecto a las categorías específicas de sistemas de IA de alto riesgo que presentan un riesgo grave en dos o más Estados miembros de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de IA prestará apoyo de coordinación a las investigaciones conjuntas.

12. Sin perjuicio de los poderes previstos en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, los proveedores concederán a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desarrollo de los sistemas de IA de alto riesgo, también, cuando proceda y con sujeción a garantías de seguridad, a través de interfaces de programación de aplicaciones (API) o de otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

13. Se concederá a las autoridades de vigilancia del mercado acceso al código fuente del sistema de IA de alto riesgo, previa solicitud motivada y solo si se cumplen las dos siguientes condiciones:

a) el acceso al código fuente es necesario para evaluar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2, y

b) se han agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o han resultado insuficientes.

14. Cualesquiera información o documentación obtenidas por las autoridades de vigilancia del mercado se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 75

Asistencia mutua, vigilancia del mercado y control de sistemas de IA de uso general

1. Cuando un sistema de IA se base en un modelo de IA de uso general y un mismo proveedor desarrolle tanto el modelo como el sistema, la Oficina de IA estará facultada para vigilar y supervisar el cumplimiento por parte de dicho sistema de IA de las obligaciones en virtud del presente Reglamento. Para llevar a cabo estas tareas de vigilancia y supervisión, la Oficina de IA tendrá todos los poderes de una autoridad prevista en la presente sección y en el Reglamento (UE) 2019/1020.

2. Cuando las autoridades de vigilancia del mercado pertinentes tengan motivos suficientes para considerar que los sistemas de IA de uso general que pueden ser utilizados directamente por los responsables del despliegue al menos para una de las finalidades clasificadas como de alto riesgo con arreglo al presente Reglamento no cumplen los requisitos establecidos en el presente Reglamento, cooperarán con la Oficina de IA para llevar a cabo evaluaciones del cumplimiento e informarán al respecto al Consejo de IA y las demás autoridades de vigilancia del mercado.

3. Cuando una autoridad de vigilancia del mercado no pueda concluir su investigación sobre el sistema de IA de alto riesgo por no poder acceder a determinada información relativa al modelo de IA de uso general, a pesar de haber realizado todos los esfuerzos adecuados para obtener esa información, podrá presentar una solicitud motivada a la Oficina de IA para que se imponga el acceso a dicha información. En tal caso, la Oficina de IA facilitará a la autoridad solicitante sin demora y, en cualquier caso en un plazo de treinta días, toda la información que la Oficina de IA considere pertinente para determinar si un sistema de IA de alto riesgo no es conforme. Las autoridades de vigilancia del mercado preservarán la confidencialidad de la información obtenida de conformidad con lo dispuesto en el artículo 78 del presente Reglamento. Se aplicará *mutatis mutandis* el procedimiento previsto en el capítulo VI del Reglamento (UE) 2019/1020.

Artículo 76

Supervisión de las pruebas en condiciones reales por las autoridades de vigilancia del mercado

1. Las autoridades de vigilancia del mercado tendrán las competencias y los poderes necesarios para garantizar que las pruebas en condiciones reales se ajusten a lo dispuesto en el presente Reglamento.

2. Cuando se realicen pruebas en condiciones reales de sistemas de IA supervisadas dentro de un espacio controlado de pruebas para la IA con arreglo al artículo 58, las autoridades de vigilancia del mercado verificarán el cumplimiento de del artículo 60 como parte de su función supervisora en el espacio controlado de pruebas para la IA. Dichas autoridades podrán permitir, según proceda, que el proveedor o proveedor potencial lleve a cabo pruebas en condiciones reales, como excepción a las condiciones establecidas en el artículo 60, apartado 4, letras f) y g).

3. Cuando una autoridad de vigilancia del mercado haya sido informada por el proveedor potencial, el proveedor o un tercero de un incidente grave o tenga otros motivos para pensar que no se cumplen las condiciones establecidas en los artículos 60 y 61, podrá adoptar una de las decisiones siguientes en su territorio, según proceda:

a) suspender o poner fin a las pruebas en condiciones reales;

b) exigir al proveedor o proveedor potencial y al responsable del despliegue o responsable del despliegue potencial que modifiquen cualquier aspecto de las pruebas en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3 del presente artículo o haya formulado una objeción en el sentido del artículo 60, apartado 4, letra b), la decisión o la objeción deberá estar motivada e indicar las vías de que dispone el proveedor o proveedor potencial para poder impugnar la decisión o la objeción.

5. En su caso, cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3, comunicará los motivos de dicha decisión a las autoridades de vigilancia del mercado de los demás Estados miembros en que se haya probado el sistema de IA de conformidad con el plan de la prueba.

Artículo 77

Poderes de las autoridades encargadas de proteger los derechos fundamentales

1. 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, incluido el derecho a la no discriminación, con respecto al uso de sistemas de IA de alto riesgo mencionados en el anexo III tendrán la facultad de solicitar cualquier documentación creada o conservada con arreglo al presente Reglamento y de acceder a ella, en un lenguaje y formato accesibles, cuando el acceso a dicha documentación sea necesario para el cumplimiento efectivo de sus mandatos, dentro de los límites de su jurisdicción. La autoridad u organismo público pertinente informará sobre cualquier solicitud de este tipo a la autoridad de vigilancia del mercado del Estado miembro que corresponda.

2. A más tardar el 2 de noviembre de 2024, cada Estado miembro designará las autoridades u organismos públicos a que se refiere el apartado 1 y los incluirá en una lista que pondrá a disposición del público. Los Estados miembros notificarán dicha lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

3. Cuando la documentación mencionada en el apartado 1 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el Derecho de la Unión en materia de protección de los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 1 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.

4. Cualquier información o documentación obtenidas por las autoridades u organismos públicos nacionales a que se refiere el apartado 1 del presente artículo con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 78.

Artículo 78

Confidencialidad

1. La Comisión, las autoridades de vigilancia del mercado, los organismos notificados y cualquier otra persona física o jurídica que participe en la aplicación del presente Reglamento, de conformidad con el Derecho de la Unión o nacional, 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 e industrial y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos mencionados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo ([57]);

b) la aplicación eficaz del presente Reglamento, en particular a efectos de investigaciones, inspecciones o auditorías;

c) los intereses de seguridad pública y nacional;

d) el desarrollo de las causas penales o los procedimientos administrativos;

e) la información clasificada con arreglo al Derecho de la Unión o nacional.

2. Las autoridades involucradas en la aplicación del presente Reglamento de conformidad con el apartado 1 solo solicitarán los datos que sean estrictamente necesarios para la evaluación del riesgo que presentan los sistemas de IA y para el ejercicio de sus competencias de conformidad con el presente Reglamento y con el Reglamento (UE) 2019/1020. Establecerán medidas adecuadas y eficaces en materia de ciberseguridad a fin de proteger la seguridad y la confidencialidad de la información y los datos obtenidos, y suprimirán los datos recopilados tan pronto como dejen de ser necesarios para los fines para los que se obtuvieron, de conformidad con el Derecho de la Unión y nacional aplicable.

3. Sin perjuicio de lo dispuesto en los apartados 1 y 2, la información intercambiada de forma confidencial entre las autoridades nacionales competentes o entre estas y la Comisión no se revelará sin consultar previamente a la autoridad nacional competente de origen y al responsable del despliegue cuando las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo utilicen los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, y dicha divulgación comprometería los intereses de seguridad pública y nacional. Este intercambio de información no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo.

Cuando las autoridades garantes del cumplimiento del Derecho, de la inmigración o del asilo sean proveedores de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, 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 74, apartados 8 y 9, 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 una habilitación de seguridad del nivel adecuado.

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

5. Cuando sea necesario y con arreglo a las disposiciones pertinentes de los acuerdos internacionales y comerciales, 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 79

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

1. Los sistemas de IA que presentan un riesgo se entenderán como «productos que presentan un riesgo» tal como se definen en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riegos que afecten a la salud, la seguridad o 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 mencionado en el apartado 1 del presente artículo, 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. Debe prestarse una especial atención a los sistemas de IA que presenten un riesgo para los colectivos vulnerables. Cuando se detecten riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 77, apartado 1, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en lo necesario con la autoridad de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1.

([57]) Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1).

Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda.

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 del presente apartado.

3. Cuando la autoridad de vigilancia del mercado considere que el incumplimiento no se limita a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que 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 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 o su puesta en servicio, para retirar el producto o el sistema de IA independiente de dicho mercado o recuperarlo. Dicha autoridad notificará estas medidas sin demora indebida a la Comisión y a los demás Estados miembros.

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

a) el no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5;

b) el incumplimiento de los requisitos establecidos en el capítulo III, sección 2, por parte de un sistema de IA de alto riesgo;

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

d) el incumplimiento del artículo 50.

7. Las autoridades de vigilancia del mercado distintas de la autoridad de vigilancia del mercado del Estado miembro que inició el procedimiento comunicarán sin demora indebida a la Comisión y a los demás Estados miembros toda medida que adopten y cualquier información adicional de que dispongan en relación con la no conformidad del sistema de IA de que se trate 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 notificación mencionada en el apartado 5 del presente artículo, ninguna autoridad de vigilancia del mercado de un Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por una autoridad de vigilancia del mercado de otro 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. El plazo de tres meses a que se refiere el presente apartado se reducirá a treinta días en caso de no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 del presente Reglamento.

9. Las autoridades de vigilancia del mercado velarán por que se adopten sin demora indebida las medidas restrictivas adecuadas respecto del producto o del sistema de IA de que se trate, tales como la retirada del producto o del sistema de IA de su mercado.

Artículo 80

Procedimiento aplicable a los sistemas de IA clasificados por el proveedor como no de alto riesgo en aplicación del anexo III

1. Cuando una autoridad de vigilancia del mercado tenga motivos suficientes para considerar que un sistema de IA que el proveedor haya clasificado como no de alto riesgo con arreglo al artículo 6, apartado 3, sí lo es, dicha autoridad realizará una evaluación del sistema de IA de que se trate por cuanto se refiere a su clasificación como sistema de IA de alto riesgo en función de las condiciones establecidas en el artículo 6, apartado 3, y las directrices de la Comisión.

2. Cuando, al realizar dicha evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA afectado es de alto riesgo, pedirá sin demora indebida al proveedor correspondiente que adopte todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento, así como que adopte las medidas correctoras adecuadas en el plazo que la autoridad de vigilancia del mercado podrá determinar.

3. Cuando la autoridad de vigilancia del mercado considere que la utilización del sistema de IA afectado no se circunscribe a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que haya exigido al proveedor que adopte.

4. El proveedor se asegurará de que se adopten todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones que se establecen en el presente Reglamento. Cuando el proveedor de un sistema de IA afectado no haga lo necesario para que cumpla dichos requisitos y obligaciones en el plazo a que se refiere el apartado 2 del presente artículo, se le impondrán multas de conformidad con el artículo 99.

5. El proveedor se asegurará de que se adopten todas las medidas correctoras adecuadas para todos los sistemas de IA afectados que haya comercializado en toda la Unión.

6. Cuando el proveedor del sistema de IA afectado no adopte las medidas correctoras adecuadas en el plazo a que se refiere el apartado 2 del presente artículo, se aplicará el artículo 79, apartados 5 a 9.

7. Cuando, al realizar la evaluación con arreglo al apartado 1 del presente artículo, la autoridad de vigilancia del mercado determine que el proveedor había clasificado erróneamente el sistema de IA como de no alto riesgo con el fin de eludir la aplicación de los requisitos establecidos en el capítulo III, sección 2, se impondrán multas al proveedor de conformidad con el artículo 99.

8. En el ejercicio de su facultad de supervisión de la aplicación del presente artículo, y de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado podrán realizar los controles pertinentes, teniendo en cuenta, en particular, la información almacenada en la base de datos de la UE a que se refiere el artículo 71 del presente Reglamento.

Artículo 81

Procedimiento de salvaguardia de la Unión

1. Cuando, en el plazo de tres meses desde la recepción de la notificación a que se refiere el artículo 79, apartado 5, o en el plazo de treinta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, la autoridad de vigilancia del mercado de un Estado miembro formule objeciones sobre una medida adoptada por otra autoridad de vigilancia del mercado, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora indebida con la autoridad de vigilancia del mercado del Estado miembro pertinente y el operador u operadores, y evaluará la medida nacional. Basándose en los resultados de la mencionada evaluación, la Comisión decidirá, en un plazo de seis meses a partir de la notificación a que se refiere el artículo 79, apartado 5, o de sesenta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, si la medida nacional está justificada y notificará su decisión a la autoridad de vigilancia del mercado del Estado miembro interesado. La Comisión informará también a las demás autoridades de vigilancia del mercado de su decisión.

2. Cuando la Comisión considere que la medida adoptada por el Estado miembro correspondiente está justificada, todos los Estados miembros se asegurarán de adoptar las medidas restrictivas adecuadas con respecto al sistema de IA de que se trate, como exigir la retirada del sistema de IA de su mercado sin demora indebida, e informarán de ello a la Comisión. Cuando la Comisión considere que la medida nacional no está justificada, el Estado miembro correspondiente retirará la medida e informará de ello a la Comisión.

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 82

Sistemas de IA conformes que presenten un riesgo

1. Si, tras efectuar una evaluación con arreglo a lo dispuesto en el artículo 79 y consultar a la autoridad pública nacional a que se refiere el artículo 77, apartado 1, la autoridad de vigilancia del mercado de un Estado miembro concluye que un sistema de IA de alto riesgo, a pesar de cumplir con el presente Reglamento, presenta sin embargo un riesgo para la salud o la seguridad de las personas, para los derechos fundamentales o para otros aspectos de protección del interés público, pedirá al operador interesado que adopte todas las medidas adecuadas para garantizar 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 sin demora indebida, dentro de un plazo que dicha autoridad podrá determinar.

2. El proveedor u otro operador pertinente se asegurará de que se adoptan medidas correctoras con respecto a todos los sistemas de IA afectados que haya comercializado en el mercado de la Unión en el plazo determinado por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. Los Estados miembros informarán inmediatamente a la Comisión y a los demás Estados miembros cuando se llegue a una conclusión en virtud del apartado 1. La información facilitada incluirá todos los detalles disponibles, en particular los datos necesarios para detectar el sistema de IA afectado y para determinar su origen y cadena de suministro, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión entablará sin demora indebida consultas con los Estados miembros afectados y los operadores pertinentes y evaluará las medidas nacionales adoptadas. Basándose en los resultados de esta evaluación, la Comisión decidirá si la medida está justificada y, en su caso, propondrá otras medidas adecuadas.

5. La Comisión comunicará inmediatamente su decisión a los Estados miembros afectados y a los operadores pertinentes. Informará asimismo a los demás Estados miembros.

Artículo 83

Incumplimiento formal

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

a) se ha colocado el marcado CE contraviniendo el artículo 48;

b) no se ha colocado el marcado CE;

c) no se ha elaborado la declaración UE de conformidad con el artículo 47;

d) no se ha elaborado correctamente la declaración UE de conformidad con el artículo 47;

e) no se ha efectuado el registro en la base de datos de la UE de conformidad con el artículo 71;

f) cuando proceda, no se ha designado a un representante autorizado;

g) no se dispone de documentación técnica.

2. Si el incumplimiento a que se refiere el apartado 1 persiste, la autoridad de vigilancia del mercado del Estado miembro de que se trate adoptará medidas adecuadas y proporcionadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o para asegurarse de que se recupera o retira del mercado sin demora.

Artículo 84

Estructuras de apoyo a los ensayos de IA de la Unión

1. La Comisión designará una o varias estructuras de apoyo a los ensayos de IA de la Unión para realizar las actividades enumeradas en el artículo 21, apartado 6, del Reglamento (UE) 2019/1020 en el ámbito de la IA.

2. Sin perjuicio de las actividades a que se refiere el apartado 1, las estructuras de apoyo a los ensayos de IA de la Unión también proporcionarán asesoramiento técnico o científico independiente a petición del Consejo de IA, la Comisión o de las autoridades de vigilancia del mercado.

SECCIÓN 4

Vías de recurso

Artículo 85

Derecho a presentar una reclamación ante una autoridad de vigilancia del mercado

Sin perjuicio de otras vías administrativas o judiciales de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente.

De conformidad con el Reglamento (UE) 2019/1020, tales reclamaciones se tendrán en cuenta a la hora de llevar a cabo actividades de vigilancia del mercado y se tramitarán de conformidad con los procedimientos específicos establecidos con este fin por las autoridades de vigilancia del mercado.

Artículo 86

Derecho a explicación de decisiones tomadas individualmente

1. Toda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

2. No se aplicará el apartado 1 a la utilización de sistemas de IA para los que existan excepciones o restricciones a la obligación prevista en dicho apartado derivadas del Derecho de la Unión o nacional de conformidad con el Derecho de la Unión.

3. El presente artículo se aplicará únicamente en la medida en que el derecho a que se refiere el apartado 1 no esté previsto de otro modo en el Derecho de la Unión.

Artículo 87

Denuncia de infracciones y protección de los denunciantes

La Directiva (UE) 2019/1937 se aplicará a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien tales infracciones.

SECCIÓN 5

Supervisión, investigación, cumplimiento y seguimiento respecto de proveedores de modelos de IA de uso general

Artículo 88

Cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general

1. La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el capítulo V, teniendo en cuenta las garantías procedimentales previstas en el artículo 94. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de las competencias de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión en virtud de los Tratados.

2. Sin perjuicio de lo dispuesto en el artículo 75, apartado 3, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las facultades previstas en la presente sección, cuando resulte necesario y proporcionado para ayudar a que se lleven a cabo las actividades de su competencia en virtud del presente Reglamento.

Artículo 89

Medidas de seguimiento

1. Con el fin de llevar a cabo los cometidos que se le atribuyen en la presente sección, la Oficina de IA podrá tomar las medidas necesarias para supervisar la aplicación y cumplimiento efectivos del presente Reglamento por parte de los proveedores de modelos de IA de uso general, incluida su observancia de los códigos de buenas prácticas aprobados.

2. Los proveedores posteriores tendrán derecho a presentar reclamaciones alegando infracciones del presente Reglamento. Las reclamaciones deberán motivarse debidamente e indicar, como mínimo:

a) el punto de contacto del proveedor del modelo de IA de uso general de que se trate;

b) una descripción de los hechos, las disposiciones del presente Reglamento afectadas y los motivos por los que el proveedor posterior considera que el proveedor del modelo de IA de uso general de que se trate ha infringido el presente Reglamento;

c) cualquier otra información que el proveedor posterior que presente la reclamación considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

Artículo 90

Alertas del grupo de expertos científicos sobre riesgos sistémicos

1. El grupo de expertos científicos podrá proporcionar alertas cualificadas a la Oficina de IA cuando tenga motivos para sospechar que:

a) un modelo de IA de uso general plantea un riesgo concreto reconocible a escala de la Unión, o

b) un modelo de IA de uso general reúne las condiciones a que se refiere el artículo 51.

2. Tras recibir dicha alerta cualificada, la Comisión podrá ejercer, a través de la Oficina de IA y tras haber informado al Consejo de IA, las facultades previstas en la presente sección con el fin de evaluar la cuestión. La Oficina de IA informará al Consejo de IA de cualquier medida que se adopte de conformidad con los artículos 91 a 94.

3. Las alertas cualificadas deberán motivarse debidamente e indicar, como mínimo:

a) el punto de contacto del proveedor del modelo de IA de uso general con riesgo sistémico de que se trate;

b) una descripción de los hechos y los motivos por los que el grupo de expertos científicos proporciona la alerta;

c) cualquier otra información que el grupo de expertos científicos considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

Artículo 91

Poderes para solicitar documentación e información

1. La Comisión podrá solicitar al proveedor del modelo de IA de uso general interesado que facilite la documentación preparada por el proveedor de conformidad con los artículos 53 y 55, o cualquier otra información que sea necesaria para evaluar el cumplimiento del presente Reglamento por parte del proveedor.

2. Antes de enviar la solicitud de información, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.

3. Cuando el grupo de expertos científicos presente la correspondiente solicitud debidamente motivada, la Comisión podrá dirigir al proveedor de un modelo de IA de uso general una solicitud de información si el acceso a dicha información resulta necesario y proporcionado para que el grupo de expertos científicos pueda llevar a cabo sus cometidos en virtud del artículo 68, apartado 2.

4. La solicitud de información indicará la base jurídica y la finalidad de la solicitud, precisará qué información se requiere, fijará el plazo en el que deberá facilitarse la información e indicará las multas que se establecen en el artículo 101 por facilitar información incorrecta, incompleta o engañosa.

5. El proveedor del modelo de IA de uso general interesado, o su representante, facilitará la información solicitada. De tratarse de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas facilitarán la información solicitada en nombre del proveedor del modelo de IA de uso general interesado. Los abogados debidamente habilitados podrán facilitar la información en nombre de sus representados. Los representados seguirán siendo, no obstante, plenamente responsables, si la información facilitada es incompleta, incorrecta o engañosa.

Artículo 92

Poderes para realizar evaluaciones

1. La Oficina de IA, previa consulta al Consejo de IA, podrá realizar evaluaciones del modelo de IA de uso general de que se trate con el fin de:

a) evaluar si el proveedor cumple sus obligaciones en virtud del presente Reglamento, cuando la información recabada con arreglo al artículo 91 resulte insuficiente, o

b) investigar riesgos sistémicos a escala de la Unión de modelos de IA de uso general con riesgo sistémico, en particular a raíz de una alerta cualificada del grupo de expertos científicos de conformidad con el artículo 90, apartado 1, letra a).

2. La Comisión podrá decidir nombrar a expertos independientes para que realicen las evaluaciones en su nombre, también expertos científicos del grupo establecido de conformidad con el artículo 68. Los expertos independientes que se nombren para realizar estas tareas cumplirán los criterios establecidos en el artículo 68, apartado 2.

3. A los efectos del apartado 1, la Comisión podrá solicitar el acceso al modelo de IA de uso general de que se trate a través de API o de otros medios y herramientas técnicos adecuados, como, por ejemplo, el código fuente.

4. La solicitud de acceso indicará la base jurídica, la finalidad y los motivos de la solicitud, y fijará el plazo durante el que deberá facilitarse el acceso y las multas que se establecen en el artículo 101 por no facilitarlo.

5. Los proveedores del modelo de IA de uso general interesados o su representante facilitarán la información solicitada. En caso de que se trate de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas, facilitarán el acceso solicitado en nombre del proveedor del modelo de IA de uso general interesado.

6. La Comisión adoptará actos de ejecución en los que se establezcan las modalidades detalladas y las condiciones de las evaluaciones, incluidas las disposiciones detalladas para la participación de expertos independientes y el procedimiento para su selección. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

7. Antes de solicitar el acceso al modelo de IA de uso general de que se trate, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general para recabar más información sobre los ensayos internos del modelo, las salvaguardias internas para prevenir los riesgos sistémicos y otros procedimientos y medidas internos que el proveedor haya adoptado para mitigar tales riesgos.

Artículo 93

Poderes para solicitar la adopción de medidas

1. Cuando resulte necesario y conveniente, la Comisión podrá solicitar a los proveedores que:

a) adopten las medidas oportunas para cumplir las obligaciones establecidas en los artículos 53 y 54;

b) apliquen medidas de reducción de riesgos cuando la evaluación realizada de conformidad con el artículo 92 apunte a que existen motivos serios y fundados de preocupación por la existencia de un riesgo sistémico a escala de la Unión;

c) restrinjan la comercialización del modelo, lo retiren o lo recuperen.

2. Antes de solicitar que se adopten medidas, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.

3. Si, durante el diálogo estructurado a que se refiere el apartado 2, el proveedor del modelo de IA de uso general con riesgo sistémico se compromete a adoptar medidas de reducción para hacer frente a un riesgo sistémico a escala de la Unión, la Comisión podrá, mediante una decisión, hacer dichos compromisos vinculantes y declarar que no hay ya motivos para actuar.

Artículo 94

Garantías procesales de los operadores económicos del modelo de IA de uso general

El artículo 18 del Reglamento (UE) 2019/1020 se aplicará *mutatis mutandis* a los proveedores del modelo de IA de uso general, sin perjuicio de las garantías procesales más específicas previstas en el presente Reglamento.

CAPÍTULO X

CÓDIGOS DE CONDUCTA Y DIRECTRICES

Artículo 95

Códigos de conducta para la aplicación voluntaria de requisitos específicos

1. La Oficina de IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, con los correspondientes mecanismos de gobernanza, destinados a fomentar la aplicación voluntaria de alguno o de todos los requisitos establecidos en el capítulo III, sección 2, a los sistemas de IA que no sean de alto riesgo, teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos.

2. La Oficina de IA y los Estados miembros facilitarán la elaboración de códigos de conducta relativos a la aplicación voluntaria, también por parte de los responsables del despliegue, de requisitos específicos para todos los sistemas de IA, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos, incluidos, entre otros pero no exclusivamente, elementos como:

a) los elementos aplicables establecidos en las Directrices éticas de la Unión para una IA fiable;

b) la evaluación y reducción al mínimo de las repercusiones de los sistemas de IA en la sostenibilidad medioambiental, también por cuanto se refiere a la programación eficiente desde el punto de vista energético y las técnicas para diseñar, entrenar y utilizar la IA de manera eficiente;

c) la promoción de la alfabetización en materia de IA, en particular en el caso de las personas que se ocupan del desarrollo, funcionamiento y utilización de la IA;

d) la facilitación de un diseño inclusivo y diverso de los sistemas de IA, por ejemplo mediante la creación de equipos de desarrollo inclusivos y diversos y la promoción de la participación de las partes interesadas en dicho proceso;

e) la evaluación y prevención de los perjuicios de los sistemas de IA para las personas vulnerables o los colectivos de personas vulnerables, también por cuanto se refiere a accesibilidad para las personas con discapacidad, así como para la igualdad de género.

3. Los códigos de conducta podrán ser elaborados por proveedores o responsables del despliegue de sistemas de IA particulares, por las organizaciones que los representen o por ambos, también con la participación de cualquier parte interesada y sus organizaciones representativas, como, por ejemplo, las organizaciones de la sociedad civil y el mundo académico. Los códigos de conducta podrán comprender uno o varios sistemas de IA en función de la similitud de la finalidad prevista de los distintos sistemas.

4. La Oficina de IA y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de las pymes, incluidas las empresas emergentes, a la hora de fomentar y facilitar la elaboración de códigos de conducta.

Artículo 96

Directrices de la Comisión sobre la aplicación del presente Reglamento

1. La Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre:

a) la aplicación de los requisitos y obligaciones a que se refieren los artículos 8 a 15 y el artículo 25;

b) las prácticas prohibidas a que se refiere el artículo 5;

c) la aplicación práctica de las disposiciones relacionadas con modificaciones sustanciales;

d) la aplicación práctica de las obligaciones de transparencia establecidas en el artículo 50;

e) información detallada sobre la relación entre el presente Reglamento y la lista de actos legislativos de armonización de la Unión enumerados en el anexo I, así como otras disposiciones de Derecho de la Unión pertinentes, también por cuanto se refiere a la coherencia en su aplicación;

f) la aplicación de la definición de sistema de IA que figura en el artículo 3, punto 1.

Al publicar estas directrices, la Comisión prestará especial atención a las necesidades de las pymes, incluidas las empresas emergentes, de las autoridades públicas locales y de los sectores que tengan más probabilidades de verse afectados por el presente Reglamento.

Las directrices a que se refiere el párrafo primero del presente apartado tendrán debidamente en cuenta el estado de la técnica generalmente reconocido en materia de IA, así como las normas armonizadas y especificaciones comunes pertinentes a que se refieren los artículos 40 y 41, o las normas armonizadas o especificaciones técnicas que se establezcan con arreglo al Derecho de armonización de la Unión.

2. A petición de los Estados miembros o de la Oficina de IA, o por propia iniciativa, la Comisión actualizará las directrices anteriormente adoptadas cuando se considere necesario.

CAPÍTULO XI

DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

Artículo 97

Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados mencionados en el artículo 6, apartado 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, se otorgan a la Comisión por un período de cinco años a partir del 1 de agosto de 2024. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes mencionada en el artículo 6, apartados 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 6, apartados 6 o 7, el artículo 7, apartados 1 o 3, el artículo 11, apartado 3, el artículo 43, apartados 5 o 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, o el artículo 53, apartados 5 o 6, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 98

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, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

CAPÍTULO XII

SANCIONES

Artículo 99

Sanciones

1. De conformidad con las condiciones previstas en el presente Reglamento, los Estados miembros establecerán el régimen de sanciones y otras medidas de ejecución, como advertencias o medidas no pecuniarias, aplicable a las infracciones del presente Reglamento que cometan los operadores y adoptarán todas las medidas necesarias para garantizar que se aplican de forma adecuada y efectiva y teniendo así en cuenta las directrices emitidas por la Comisión con arreglo al artículo 96. Tales sanciones serán efectivas, proporcionadas y disuasorias. Tendrán en cuenta los intereses de las pymes, incluidas las empresas emergentes, así como su viabilidad económica.

2. Los Estados miembros comunicarán a la Comisión, sin demora y, como muy tarde, en la fecha de aplicación las normas referentes a las sanciones y otras medidas de ejecución mencionadas en el apartado 1 y la informará, sin demora, de toda modificación de dichas normas.

3. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 35 000 000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

4. El incumplimiento de cualquiera de las disposiciones que figuran a continuación en relación con los operadores o los organismos notificados, distintas de los mencionados en el artículo 5, estará sujeto a multas administrativas de hasta 15 000 000 EUR o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior:

a) las obligaciones de los proveedores con arreglo al artículo 16;

b) las obligaciones de los representantes autorizados con arreglo al artículo 22;

c) las obligaciones de los importadores con arreglo al artículo 23;

d) las obligaciones de los distribuidores con arreglo al artículo 24;

e) las obligaciones de los responsables del despliegue con arreglo al artículo 26;

f) los requisitos y obligaciones de los organismos notificados con arreglo al artículo 31, al artículo 33, apartados 1, 3 y 4, o al artículo 34;

g) las obligaciones de transparencia de los proveedores y responsables del despliegue con arreglo al artículo 50.

5. La presentación de información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 7 500 000 EUR o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

6. En el caso de las pymes, incluidas las empresas emergentes, cada una de las multas a que se refiere el presente artículo podrá ser por el porcentaje o el importe a que se refieren los apartados 3, 4 y 5, según cuál de ellos sea menor.

7. 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, en su caso, se tendrá en cuenta lo siguiente:

a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA y, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;

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

c) si otras autoridades han impuesto ya multas administrativas al mismo operador por infracciones de otros actos legislativos nacionales o de la Unión, cuando dichas infracciones se deriven de la misma actividad u omisión que constituya una infracción pertinente del presente Reglamento;

d) el tamaño, el volumen de negocios anual y la cuota de mercado del operador que comete la infracción;

e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción;

f) el grado de cooperación con las autoridades nacionales competentes con el fin de subsanar la infracción y mitigar sus posibles efectos adversos;

g) el grado de responsabilidad del operador, teniendo en cuenta las medidas técnicas y organizativas aplicadas por este;

h) la forma en que las autoridades nacionales competentes tuvieron conocimiento de la infracción, en particular si el operador notificó la infracción y, en tal caso, en qué medida;

i) la intencionalidad o negligencia en la infracción;

j) las acciones emprendidas por el operador para mitigar los perjuicios sufridos por las personas afectadas.

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

9. 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.

10. El ejercicio de poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y nacional, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

11. Los Estados miembros informarán anualmente a la Comisión de las multas administrativas que hayan impuesto durante ese año de conformidad con el presente artículo y de cualquier litigio o proceso judicial relacionados.

Artículo 100

Multas administrativas a instituciones, órganos y organismos de la Unión

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, órganos y 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, teniendo en cuenta la finalidad del sistema de IA de que se trate, así como, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;

b) el grado de responsabilidad de la institución, órgano u organismo de la Unión, teniendo en cuenta las medidas técnicas y organizativas aplicadas;

c) las acciones emprendidas por la institución, órgano u organismo de la Unión para mitigar los perjuicios sufridos por las personas afectadas;

d) el grado de cooperación con el Supervisor Europeo de Protección de Datos con el fin de subsanar 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, órgano u organismo de la Unión de que se trate en relación con el mismo asunto;

e) toda infracción anterior similar cometida por la institución, órgano u organismo de la Unión;

f) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución, órgano u organismo de la Unión notificó la infracción y, en tal caso, en qué medida;

g) el presupuesto anual de la institución, órgano u organismo de la Unión.

2. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 1 500 000 EUR.

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento, distintos de los previstos en el artículo 5, estará sujeto a multas administrativas de hasta 750 000 EUR.

4. Antes de tomar ninguna decisión en virtud del presente artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución, órgano 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 los que las partes afectadas hayan podido manifestarse. Los denunciantes, si los hay, participarán estrechamente en el 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 contribuirá al presupuesto general de la Unión. Las multas no afectarán al funcionamiento efectivo de la institución, órgano u organismo de la Unión sancionado.

7. El Supervisor Europeo de Protección de Datos informará anualmente a la Comisión de las multas administrativas que haya impuesto en virtud del presente artículo y de cualquier litigio o proceso judicial que haya iniciado.

Artículo 101

Multas a proveedores de modelos de IA de uso general

1. La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15 000 000 EUR, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia:

a) infringieron las disposiciones pertinentes del presente Reglamento;

b) no atendieron una solicitud de información o documentos con arreglo al artículo 91, o han facilitado información inexacta, incompleta o engañosa;

c) incumplieron una medida solicitada en virtud del artículo 93;

d) no dieron acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación con arreglo al artículo 92.

Al fijar el importe de la multa o de la multa coercitiva, se tomarán en consideración la naturaleza, gravedad y duración de la infracción, teniendo debidamente en cuenta los principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos de conformidad con el artículo 93, apartado 3, y en los códigos de buenas prácticas pertinentes previstos en el artículo 56.

2. Antes de adoptar una decisión con arreglo al apartado 1, la Comisión comunicará sus conclusiones preliminares al proveedor del modelo de IA de uso general o del modelo de IA y le dará la oportunidad de ser oído.

3. Las multas impuestas de conformidad con el presente artículo serán efectivas, proporcionadas y disuasorias.

4. La información sobre las multas impuestas en virtud del presente artículo también se comunicará al Consejo de IA, según proceda.

5. El Tribunal de Justicia de la Unión Europea tendrá plena competencia jurisdiccional para examinar las decisiones de imposición de una multa adoptadas por la Comisión en virtud del presente artículo. Podrá anular, reducir o incrementar la cuantía de la multa impuesta.

6. La Comisión adoptará actos de ejecución que contengan disposiciones detalladas y garantías procesales para los procedimientos con vistas a la posible adopción de decisiones con arreglo al apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO XIII

DISPOSICIONES FINALES

Artículo 102

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) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 103

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) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 104

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) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 105

Modificación de la Directiva 2014/90/UE

En el artículo 8 de la Directiva 2014/90/UE, se añade el apartado siguiente:

«5. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), la Comisión tendrá en cuenta los requisitos establecidos en el capítulo III, sección 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) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 106

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) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 107

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) 2024/… del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 108

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) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

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) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 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) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 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) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

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

«Al adoptar dichos actos de ejecución relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 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 sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

Artículo 109

Modificación del Reglamento (UE) 2019/2144

En el artículo 11 del Reglamento (UE) 2019/2144, se añade el párrafo siguiente:

«3. Al adoptar actos de ejecución en virtud del apartado 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 110

Modificación de la Directiva (UE) 2020/1828

En el anexo I de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo ([58]) se añade el punto siguiente:

«68) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 1689, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artículo 111

Sistemas de IA ya introducidos en el mercado o puestos en servicio y modelos de IA de uso general ya introducidos en el mercado

1. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, apartado 3, letra a), los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo X que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2027 deberán estar en conformidad con el presente Reglamento a más tardar el 31 de diciembre de 2030.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta en la evaluación de cada sistema informático de gran magnitud establecido en virtud de los actos jurídicos enumerados en el anexo X que se efectúe de conformidad con lo dispuesto en dichos actos jurídicos y cuando dichos actos jurídicos hayan sido sustituidos o modificados.

2. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, apartado 3, letra a), el presente Reglamento se aplicará a los operadores de sistemas de IA de alto riesgo, distintos de los mencionados en el apartado 1 del presente artículo, que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2026 únicamente si, a partir de esa fecha, dichos sistemas se ven sometidos a cambios significativos en su diseño. En cualquier caso, los proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas adoptarán las medidas necesarias para cumplir los requisitos y obligaciones del presente Reglamento a más tardar el 2 de agosto de 2030.

3. Los proveedores de modelos de IA de uso general que se hayan introducido en el mercado antes del 2 de agosto de 2025 adoptarán las medidas necesarias para cumplir las obligaciones establecidas en el presente Reglamento a más tardar el 2 de agosto de 2027.

([58]) Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

Artículo 112

Evaluación y revisión

1. La Comisión evaluará la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas previstas en el artículo 5 una vez al año a partir de la entrada en vigor del presente Reglamento y hasta el final del período de delegación de poderes previsto en el artículo 97. La Comisión presentará las conclusiones de dicha evaluación al Parlamento Europeo y al Consejo.

2. A más tardar el 2 de agosto de 2028, y posteriormente cada cuatro años, la Comisión evaluará los puntos siguientes e informará de ello al Parlamento Europeo y al Consejo:

a) la necesidad de ampliar los ámbitos enumerados en el anexo III o de añadir nuevos ámbitos;

b) la necesidad de modificar la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50;

c) la necesidad de mejorar la eficacia del sistema de supervisión y gobernanza.

3. A más tardar el 2 de agosto de 2029, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. El informe incluirá una evaluación de la estructura de control del cumplimiento y de la posible necesidad de que una agencia de la Unión resuelva las deficiencias detectadas. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento. Los informes se harán públicos.

4. En los informes mencionados en el apartado 2 se prestará una atención especial a lo siguiente:

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

b) el estado de las sanciones, en particular, de las multas administrativas a que se refiere el artículo 99, apartado 1, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento;

c) las normas armonizadas adoptadas y las especificaciones comunes desarrolladas en apoyo del presente Reglamento;

d) el número de empresas que entran en el mercado después de que se empiece a aplicar el presente Reglamento y, de entre ellas, el número de pymes.

5. A más tardar el 2 de agosto de 2028, la Comisión evaluará el funcionamiento de la Oficina de IA, si se le han otorgado poderes y competencias suficientes para desempeñar sus funciones, y si sería pertinente y necesario para la correcta aplicación y ejecución del presente Reglamento mejorar la Oficina de IA y sus competencias de ejecución, así como aumentar sus recursos. La Comisión presentará un informe sobre su evaluación al Parlamento Europeo y al Consejo.

6. A más tardar el 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión presentará un informe sobre la revisión de los avances en la elaboración de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general y evaluará la necesidad de medidas o acciones adicionales, incluidas medidas o acciones vinculantes. Este informe se remitirá al Parlamento Europeo y al Consejo y se hará público.

7. A más tardar el 2 de agosto de 2028 y posteriormente cada tres años, la Comisión evaluará la incidencia y la eficacia de los códigos de conducta voluntarios por lo que respecta a promover la aplicación de los requisitos establecidos en el capítulo III, sección 2, a sistemas de IA que no sean de alto riesgo y, en su caso, de otros requisitos adicionales aplicables a los sistemas de IA que no sean sistemas de IA de alto riesgo, como, por ejemplo, requisitos relativos a la sostenibilidad medioambiental.

8. A efectos de lo dispuesto en los apartados 1 a 7, el Consejo de IA, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión, cuando así lo solicite, y sin demora indebida.

9. Al llevar a cabo las evaluaciones y revisiones mencionadas en los apartados 1 a 7, la Comisión tendrá en cuenta las posiciones y conclusiones del Consejo de IA, el Parlamento Europeo, el Consejo y los demás organismos o fuentes pertinentes.

10. 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 el efecto de los sistemas de IA en la salud y la seguridad y en los derechos fundamentales, y a la vista de los avances en la sociedad de la información.

11. Para orientar las evaluaciones y revisiones a que se refieren los apartados 1 a 7 del presente artículo, la Oficina de IA se encargará de desarrollar una metodología objetiva y participativa para la evaluación de los niveles de riesgo a partir de los criterios expuestos en los artículos pertinentes y la inclusión de nuevos sistemas en:

a) la lista establecida en el anexo III, incluida la ampliación de los ámbitos existentes o la inclusión de nuevos ámbitos en dicho anexo;

b) la lista de prácticas prohibidas establecida en el artículo 5, y

c) la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50.

12. Las modificaciones del presente Reglamento con arreglo al apartado 10, o los actos delegados o de ejecución pertinentes, que afecten a los actos legislativos de armonización de la Unión sectoriales que se enumeran en el anexo I, sección B, tendrán en cuenta las particularidades normativas de cada sector y los mecanismos de gobernanza, evaluación de la conformidad y ejecución vigentes, así como las autoridades establecidas en ellos.

13. A más tardar el 2 de agosto de 2031, la Comisión evaluará la ejecución del presente Reglamento e informará al respecto al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, teniendo en cuenta los primeros años de aplicación del presente Reglamento. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento en lo que respecta a la estructura de ejecución y a la necesidad de que una agencia de la Unión resuelva las deficiencias detectadas.

Artículo 113

Entrada en vigor y aplicación

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

Será aplicable a partir del 2 de agosto de 2026.

No obstante:

a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025;

b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;

c) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

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

Hecho en Bruselas, el 13 de junio de 2024.

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta	*El Presidente*
R. METSOLA	M. MICHEL

ANEXO I

Lista de actos legislativos de armonización de la Unión

Sección A — Lista de actos legislativos de armonización de la Unión basados en el nuevo marco legislativo

1. Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24)

2. Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes (DO L 170 de 30.6.2009, p. 1)

3. Directiva 2013/53/UE del Parlamento Europeo y del Consejo, de 20 de noviembre de 2013, relativa a las embarcaciones de recreo y a las motos acuáticas, y por la que se deroga la Directiva 94/25/CE (DO L 354 de 28.12.2013, p. 90)

4. Directiva 2014/33/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de ascensores y componentes de seguridad para ascensores (DO L 96 de 29.3.2014, p. 251)

5. Directiva 2014/34/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas (DO L 96 de 29.3.2014, p. 309)

6. Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62)

7. Directiva 2014/68/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos a presión (DO L 189 de 27.6.2014, p. 164)

8. Reglamento (UE) 2016/424 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a las instalaciones de transporte por cable y por el que se deroga la Directiva 2000/9/CE (DO L 81 de 31.3.2016, p. 1)

9. Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a los equipos de protección individual y por el que se deroga la Directiva 89/686/CEE del Consejo (DO L 81 de 31.3.2016, p. 51)

10. Reglamento (UE) 2016/426 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre los aparatos que queman combustibles gaseosos y por el que se deroga la Directiva 2009/142/CE (DO L 81 de 31.3.2016, p. 99)

11. 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)

12. 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)

Sección B — Lista de otros actos legislativos de armonización de la Unión

13. 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)

14. 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)

15. 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)

16. 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)

17. 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)

18. 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 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)

19. 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 de 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)

20. 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 y (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), en la medida en que afecte al diseño, la producción y la introducción en el mercado de aeronaves a que se refiere el artículo 2, apartado 1, letras a) y b), por lo que respecta a las aeronaves no tripuladas y sus motores, hélices, componentes y equipos para controlarlas a distancia

ANEXO II

Lista de los delitos a que se refiere el artículo 5, apartado 1, párrafo primero, letra h), inciso iii)

Delitos a que se refiere el artículo 5, apartado 1, párrafo primero, letra h), inciso iii):

— terrorismo,

— trata de seres humanos,

— explotación sexual de menores y pornografía infantil,

— tráfico ilícito de estupefacientes o sustancias psicotrópicas,

— tráfico ilícito de armas, municiones y explosivos,

— homicidio voluntario, agresión con lesiones graves,

— tráfico ilícito de órganos o tejidos humanos,

— tráfico ilícito de materiales nucleares o radiactivos,

— secuestro, detención ilegal o toma de rehenes,

— delitos que son competencia de la Corte Penal Internacional,

— secuestro de aeronaves o buques,

— violación,

— delitos contra el medio ambiente,

— robo organizado o a mano armada,

— sabotaje,

— participación en una organización delictiva implicada en uno o varios de los delitos enumerados en esta lista.

ANEXO III

Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2

Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA que formen parte de cualquiera de los ámbitos siguientes:

1. Biometría, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

   a) Sistemas de identificación biométrica remota

      Quedan excluidos los sistemas de IA destinados a ser utilizados con fines de verificación biométrica cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser

   b) Sistemas de IA destinados a ser utilizados para la categorización biométrica en función de atributos o características sensibles o protegidos basada en la inferencia de dichos atributos o características

   c) Sistemas de IA destinados a ser utilizados para el reconocimiento de emociones

2. Infraestructuras críticas: Sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad

3. Educación y formación profesional:

   a) Sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión de personas físicas a centros educativos y de formación profesional a todos los niveles o para distribuir a las personas físicas entre dichos centros

   b) Sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en centros educativos y de formación profesional a todos los niveles

   c) Sistemas de IA destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles

   d) Sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante los exámenes en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles

4. Empleo, gestión de los trabajadores y acceso al autoempleo:

   a) Sistemas de IA destinados a ser utilizados para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos

   b) Sistemas de IA destinados a ser utilizados para tomar decisiones que afecten a las condiciones de las relaciones de índole laboral o a la promoción o rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales o para supervisar y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones

5. Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones:

   a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución

   b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros

   c) Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud

d) Sistemas de IA destinados a ser utilizados para la evaluación y la clasificación de las llamadas de emergencia realizadas por personas físicas o para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo, policía, bomberos y servicios de asistencia médica, y en sistemas de triaje de pacientes en el contexto de la asistencia sanitaria de urgencia

6. Garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

a) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, o en su nombre, para evaluar el riesgo de que una persona física sea víctima de delitos

b) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho como polígrafos o herramientas similares

c) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos

d) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito atendiendo no solo a la elaboración de perfiles de personas físicas mencionada en el artículo 3, punto 4, de la Directiva (UE) 2016/680 o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos

e) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para elaborar perfiles de personas físicas, como se menciona en el artículo 3, punto 4, de la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de delitos

7. Migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, como polígrafos o herramientas similares

b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para evaluar un riesgo, por ejemplo, un riesgo para la seguridad, la salud o de migración irregular, que plantee una persona física que tenga la intención de entrar en el territorio de un Estado miembro o haya entrado en él

c) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado o permiso de residencia y las reclamaciones conexas con el fin de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, con inclusión de la evaluación conexa de la fiabilidad de las pruebas

d) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, en el contexto de la migración, el asilo o la gestión del control fronterizo, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje

8. Administración de justicia y procesos democráticos:

a) Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios;

b) Sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos. Quedan excluidos los sistemas de IA a cuyos resultados de salida no estén directamente expuestos las personas físicas, como las herramientas utilizadas para organizar, optimizar o estructurar campañas políticas desde un punto de vista administrativo o logístico.

ANEXO IV

Documentación técnica a que se refiere el artículo 11, apartado 1

La documentación técnica a que se refiere el artículo 11, apartado 1, incluirá como mínimo la siguiente información, aplicable al sistema de IA pertinente:

1. Una descripción general del sistema de IA que incluya:

   a) su finalidad prevista, el nombre del proveedor y la versión del sistema de tal manera que se refleje su relación con versiones anteriores;

   b) la manera en que el sistema de IA interactúa o puede utilizarse para interactuar con *hardware* o *software*, también con otros sistemas de IA, que no formen parte del propio sistema de IA, cuando proceda;

   c) las versiones de *software* o *firmware* pertinentes y todo requisito relacionado con la actualización de versiones;

   d) la descripción de todas las formas en que el sistema de IA se introduce en el mercado o se pone en servicio, como paquetes de software integrados en el *hardware*, descargas o API;

   e) la descripción del *hardware* en el que está previsto que se ejecute el sistema de IA;

   f) en el caso de que el sistema de IA sea un componente de un producto, fotografías o ilustraciones de las características exteriores, el marcado y la configuración interna de dicho producto;

   g) una descripción básica de la interfaz de usuario facilitada al responsable del despliegue;

   h) instrucciones de uso para el responsable del despliegue y una descripción básica de la interfaz de usuario facilitada al responsable del despliegue, cuando proceda.

2. Una descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, incluidos:

   a) los métodos y las medidas adoptados para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas previamente entrenados facilitados por terceros y la manera en que han sido utilizados, integrados o modificados por el proveedor;

   b) las especificaciones de diseño del sistema, a saber, la lógica general del sistema de IA y de los algoritmos; las decisiones clave de diseño, incluidos la lógica y los supuestos de los que se ha partido, también con respecto a las personas o colectivos de personas en relación con los que está previsto que se utilice el sistema; las principales decisiones de clasificación; aquello que el sistema está diseñado para optimizar y la pertinencia de los diversos parámetros; la descripción de los resultados de salida esperados del sistema y la calidad de dichos resultados; las decisiones adoptadas acerca de cualquier posible concesión con respecto a las soluciones técnicas adoptadas para dar cumplimiento a los requisitos establecidos en el capítulo III, sección 2;

   c) la arquitectura del sistema, con una explicación de la manera en que los componentes del *software* se utilizan o enriquecen mutuamente y de la manera en que se integran en el procesamiento general; los recursos informáticos utilizados para desarrollar, entrenar, probar y validar el sistema de IA;

   d) cuando proceda, los requisitos en materia de datos, en forma de fichas técnicas que describan las metodologías y técnicas de entrenamiento, así como los conjuntos de datos de entrenamiento utilizados, e incluyan una descripción general de dichos conjuntos de datos e información acerca de su procedencia, su alcance y sus características principales; la manera en que se obtuvieron y seleccionaron los datos; los procedimientos de etiquetado (p. ej., para el aprendizaje supervisado) y las metodologías de depuración de datos (p. ej., la detección de anomalías);

   e) una evaluación de las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluida una evaluación de las medidas técnicas necesarias para facilitar la interpretación de los resultados de salida de los sistemas de IA por parte de los responsables del despliegue, con arreglo al artículo 13, apartado 3, letra d);

   f) en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su funcionamiento, junto con toda la información pertinente relativa a las soluciones técnicas adoptadas con el objetivo de garantizar la conformidad permanente del sistema de IA con los requisitos pertinentes establecidos en el capítulo III, sección 2;

   g) los procedimientos de validación y prueba utilizados, incluida la información acerca de los datos de validación y prueba empleados y sus características principales; los parámetros utilizados para medir la precisión, la solidez y el cumplimiento de otros requisitos pertinentes establecidos en el capítulo III, sección 2, así como los efectos potencialmente discriminatorios; los archivos de registro de las pruebas y todos los informes de las pruebas fechados y firmados por las personas responsables, también en lo que respecta a los cambios predeterminados a que se refiere la letra f);

h) las medidas de ciberseguridad adoptadas.

3. Información detallada acerca de la supervisión, el funcionamiento y el control del sistema de IA, en particular con respecto a sus capacidades y limitaciones de funcionamiento, incluidos los niveles de precisión para las personas o colectivos de personas específicos en relación con los que está previsto que se utilice el sistema y el nivel general de precisión esperado en relación con su finalidad prevista; los resultados no deseados previsibles y las fuentes de riesgo para la salud y la seguridad, los derechos fundamentales y la discriminación, en vista de la finalidad prevista del sistema de IA; las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA por parte de los responsables del despliegue; las especificaciones de los datos de entrada, según proceda.

4. Una descripción de la idoneidad de los parámetros de rendimiento para el sistema de IA concreto.

5. Una descripción detallada del sistema de gestión de riesgos con arreglo al artículo 9.

6. Una descripción de los cambios pertinentes realizados por el proveedor en el sistema a lo largo de su ciclo de vida.

7. Una lista de las normas armonizadas, aplicadas total o parcialmente, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*; cuando no se hayan aplicado normas armonizadas, una descripción detallada de las soluciones adoptadas para cumplir los requisitos establecidos en el capítulo III, sección 2, incluida una lista de otras normas y especificaciones técnicas pertinentes que se hayan aplicado.

8. Una copia de la declaración UE de conformidad de conformidad con el artículo 47.

9. Una descripción detallada del sistema establecido para evaluar el funcionamiento del sistema de IA en la fase posterior a la comercialización, de conformidad con el artículo 72, incluido el plan de vigilancia poscomercialización a que se refiere el artículo 72, apartado 3.

ANEXO V

Declaración UE de conformidad

La declaración UE de conformidad a que se hace referencia en el artículo 47 contendrá toda la información siguiente:

1. El nombre y tipo del sistema de IA, y toda referencia inequívoca adicional que permita la identificación y trazabilidad del sistema de IA.
2. El nombre y la dirección del proveedor o, en su caso, de su representante autorizado.
3. La afirmación de que la declaración UE de conformidad con el artículo 47 se expide bajo la exclusiva responsabilidad del proveedor.
4. La declaración de que el sistema de IA es conforme con el presente Reglamento y, en su caso, con cualquier otra disposición de Derecho de la Unión pertinente que disponga la expedición de la declaración UE de conformidad con el artículo 47.
5. Cuando un sistema de IA implique el tratamiento de datos personales, la declaración de que el sistema de IA se ajusta al Reglamento (UE) 2016/679, al Reglamento (UE) 2018/1725 y a la Directiva (UE) 2016/680.
6. Referencias a todas las normas armonizadas pertinentes que se hayan aplicado o a cualquier otra especificación común respecto de la que se declara la conformidad.
7. En su caso, el nombre y el número de identificación del organismo notificado, una descripción del procedimiento de evaluación de la conformidad que se haya seguido y la identificación del certificado expedido.
8. El lugar y la fecha de expedición de la declaración, el nombre y el cargo de la persona que la firme, la indicación de la persona en cuyo nombre o por cuya cuenta firma la declaración y la firma.

ANEXO VI

Procedimiento de evaluación de la conformidad fundamentado en un control interno

1. El procedimiento de evaluación de la conformidad fundamentado en un control interno es el procedimiento de evaluación de la conformidad basado en los puntos 2, 3 y 4.

2. El proveedor comprueba que el sistema de gestión de la calidad establecido cumple los requisitos establecidos en el artículo 17.

3. El proveedor examina la información de la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos en el capítulo III, sección 2.

4. Asimismo, el proveedor comprueba que el proceso de diseño y desarrollo del sistema de IA y la vigilancia poscomercialización del mismo a que se refiere el artículo 72 son coherentes con la documentación técnica.

ANEXO VII

Conformidad fundamentada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica

1. Introducción

La conformidad fundamentada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 5.

2. Presentación general

El sistema de gestión de la calidad aprobado en relación con el diseño, el desarrollo y las pruebas de los sistemas de IA con arreglo al artículo 17 se examinará de conformidad con el punto 3 y será objeto de vigilancia con arreglo a lo establecido en el punto 5. La documentación técnica del sistema de IA se examinará de conformidad con el punto 4.

3. Sistema de gestión de la calidad

3.1. La solicitud del proveedor incluirá:

a) el nombre y la dirección del proveedor y, si es el representante autorizado quien presenta la solicitud, también su nombre y dirección;

b) la lista de los sistemas de IA a los que se aplica el mismo sistema de gestión de la calidad;

c) la documentación técnica de cada sistema de IA al que se aplica el mismo sistema de gestión de la calidad;

d) la documentación relativa al sistema de gestión de la calidad, que cubrirá todos los aspectos enumerados en el artículo 17;

e) una descripción de los procedimientos establecidos para garantizar que el sistema de gestión de la calidad sigue siendo adecuado y eficaz;

f) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de gestión de la calidad será evaluado por el organismo notificado, que determinará si cumple los requisitos especificados en el artículo 17.

La decisión se notificará al proveedor o a su representante autorizado.

La notificación incluirá las conclusiones de la evaluación del sistema de gestión de la calidad y una decisión motivada sobre la evaluación.

3.3. El proveedor continuará aplicando y manteniendo el sistema de gestión de la calidad aprobado de forma que siga siendo adecuado y eficaz.

3.4. El proveedor comunicará al organismo notificado toda modificación prevista del sistema de gestión de la calidad aprobado o de la lista de sistemas de IA a los que este se aplica.

El organismo notificado examinará los cambios propuestos y decidirá si el sistema de gestión de la calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2 o si es necesario realizar una nueva evaluación.

El organismo notificado notificará su decisión al proveedor. La notificación incluirá las conclusiones del examen de los cambios y una decisión motivada sobre la evaluación.

4. Control de la documentación técnica

4.1. Además de la solicitud a que se refiere el punto 3, el proveedor presentará una solicitud ante el organismo notificado de su elección para la evaluación de la documentación técnica relativa al sistema de IA que el proveedor pretenda introducir en el mercado o poner en servicio y al que se aplique el sistema de gestión de la calidad mencionado en el punto 3.

4.2. La solicitud incluirá:

a) el nombre y la dirección del proveedor;

b) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado;

c) la documentación técnica prevista en el anexo IV.

4.3. El organismo notificado examinará la documentación técnica. Cuando proceda, y en la medida en que sea necesario para el desempeño de sus tareas, se concederá al organismo notificado pleno acceso a los conjuntos de datos de entrenamiento, validación y prueba utilizados, también, cuando proceda y con sujeción a garantías de seguridad, a través de API u otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

4.4. Al examinar la documentación técnica, el organismo notificado podrá exigir que el proveedor facilite más pruebas justificativas o que lleve a cabo pruebas adicionales para que pueda evaluarse adecuadamente la conformidad del sistema de IA con los requisitos establecidos en el capítulo III, sección 2. Cuando el organismo notificado no quede satisfecho con las pruebas realizadas por el proveedor, efectuará él mismo directamente las pruebas adecuadas, según proceda.

4.5. Asimismo, se concederá al organismo notificado acceso al modelo de entrenamiento y al modelo entrenado del sistema de IA, con sus correspondientes parámetros, para, en caso necesario, una vez se hayan agotado y hayan demostrado ser insuficientes todas las demás vías razonables para verificar la conformidad, y previa solicitud motivada, evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2. Dicho acceso estará sujeto al Derecho de la Unión vigente relativo a la protección de la propiedad intelectual e industrial y los secretos comerciales.

4.6. Se notificará la decisión del organismo notificado al proveedor o a su representante autorizado. La notificación incluirá las conclusiones de la evaluación de la documentación técnica y una decisión motivada sobre la evaluación.

Cuando el sistema de IA cumpla los requisitos establecidos en el capítulo III, sección 2, el organismo notificado expedirá un certificado de la Unión de evaluación de la documentación técnica. Dicho certificado indicará el nombre y la dirección del proveedor, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para identificar el sistema de IA.

El certificado y sus anexos contendrán toda la información pertinente para poder evaluar la conformidad del sistema de IA y permitir el control del sistema de IA mientras esté en uso, cuando proceda.

Cuando el sistema de IA no cumpla los requisitos establecidos en el capítulo III, sección 2, el organismo notificado denegará la expedición del certificado de la Unión de evaluación de la documentación técnica e informará de ello al solicitante, motivando detalladamente su decisión.

Cuando el sistema de IA no cumpla los requisitos relativos a los datos utilizados para su entrenamiento, será necesario llevar a cabo un nuevo entrenamiento del sistema antes de solicitar una nueva evaluación de la conformidad. En este caso, la decisión motivada sobre la evaluación del organismo notificado que deniegue la expedición del certificado de la Unión de evaluación de la documentación técnica contendrá consideraciones específicas relativas a la calidad de los datos utilizados para entrenar el sistema de IA, en particular acerca de los motivos del incumplimiento.

4.7. Todo cambio del sistema de IA que pueda afectar a su cumplimiento de los requisitos o su finalidad prevista será evaluado por el organismo notificado que haya expedido el certificado de la Unión de evaluación de la documentación técnica. El proveedor informará a dicho organismo notificado de su intención de introducir cualquiera de los cambios previamente mencionados o de si tiene constancia de que se hayan producido tales cambios. El organismo notificado evaluará los cambios previstos y decidirá si estos requieren una nueva evaluación de la conformidad con arreglo al artículo 43, apartado 4, o si pueden ser objeto de un suplemento al certificado de la Unión de evaluación de la documentación técnica. En este último caso, el organismo notificado evaluará los cambios, notificará su decisión al proveedor y, si aprueba los cambios, expedirá un suplemento al certificado de la Unión de evaluación de la documentación técnica.

5. Vigilancia del sistema de gestión de la calidad aprobado

5.1. La finalidad de la vigilancia por parte del organismo notificado a que se refiere el punto 3 es asegurarse de que el proveedor cumple debidamente las condiciones del sistema de gestión de la calidad aprobado.

5.2. A efectos de la evaluación, el proveedor dará acceso al organismo notificado a las instalaciones donde se estén diseñando, desarrollando o probando los sistemas de IA. Además, el proveedor facilitará al organismo notificado toda la información necesaria.

5.3. El organismo notificado realizará auditorías periódicas para asegurarse de que el proveedor mantiene y aplica el sistema de gestión de la calidad, y le entregará un informe de la auditoría. En el marco de dichas auditorías, el organismo notificado podrá efectuar más pruebas de los sistemas de IA para los que se hayan expedido certificados de la Unión de evaluación de la documentación técnica.

ANEXO VIII

Información que debe presentarse para la inscripción en el registro de sistemas de IA de alto riesgo de conformidad con el artículo 49

Sección A — Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 1

Con respecto a los sistemas de IA de alto riesgo que vayan a inscribirse en el registro de conformidad con el artículo 49, apartado 1, se facilitará y se actualizará debidamente la información siguiente:

1. El nombre, la dirección y los datos de contacto del proveedor.
2. Cuando sea otra persona la que presente la información en nombre del proveedor, el nombre, dirección y datos de contacto de dicha persona.
3. El nombre, la dirección y los datos de contacto del representante autorizado, en su caso.
4. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.
5. La descripción de la finalidad prevista del sistema de IA y de los componentes y funciones que se apoyan a través del mismo.
6. Una descripción sencilla y concisa de la información que utiliza el sistema (datos, entradas) y su lógica de funcionamiento.
7. La situación del sistema de IA (comercializado o puesto en servicio, ha dejado de comercializarse o de estar en servicio, recuperado).
8. El tipo, el número y la fecha de caducidad del certificado expedido por el organismo notificado y el nombre o número de identificación de dicho organismo notificado, cuando proceda.
9. Una copia escaneada del certificado a que se refiere el punto 8, cuando proceda.
10. Todo Estado miembro en el que el sistema de IA se haya introducido en el mercado, puesto en servicio o comercializado en la Unión.
11. Una copia de la declaración UE de conformidad a que se refiere el artículo 47.
12. Las instrucciones de uso electrónicas. No se facilitará esta información en el caso de los sistemas de IA de alto riesgo en los ámbitos de la garantía del cumplimiento del Derecho o la migración, el asilo y la gestión del control fronterizo a que se refiere el anexo III, puntos 1, 6 y 7.
13. Una URL para obtener información adicional (opcional).

Sección B — Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 2

Con respecto a los sistemas de IA que vayan a inscribirse en el registro de conformidad con el artículo 49, apartado 2, se facilitará y se actualizará debidamente la información siguiente:

1. El nombre, la dirección y los datos de contacto del proveedor.
2. Cuando sea otra persona la que presente la información en nombre del proveedor, el nombre, dirección y datos de contacto de dicha persona.
3. El nombre, la dirección y los datos de contacto del representante autorizado, en su caso.
4. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.
5. La descripción de la finalidad prevista del sistema de IA.
6. La condición o condiciones previstas en el artículo 6, apartado 3, con arreglo a las cuales se considera que el sistema de IA no es de alto riesgo.
7. Un breve resumen de los motivos por los que se considera que el sistema de IA no es de alto riesgo en aplicación del procedimiento previsto en el artículo 6, apartado 3.
8. La situación del sistema de IA (comercializado o puesto en servicio, ha dejado de comercializarse o de estar en servicio, recuperado).
9. Todo Estado miembro en el que el sistema de IA se haya introducido en el mercado, puesto en servicio o comercializado en la Unión.

Sección C — Información que deben presentar los responsables del despliegue de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 3

Con respecto a los sistemas de IA de alto riesgo que vayan a inscribirse en el registro de conformidad con el artículo 49, apartado 3, se facilitará y se actualizará debidamente la información siguiente:

1. El nombre, la dirección y los datos de contacto del responsable del despliegue.
2. El nombre, la dirección y los datos de contacto de la persona que presente la información en nombre del responsable del despliegue.
3. La URL de entrada del sistema de IA en la base de datos de la UE por parte de su proveedor.
4. Un resumen de las conclusiones de la evaluación de impacto relativa a los derechos fundamentales realizada de conformidad con el artículo 27.
5. Un resumen de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, tal como se especifica en el artículo 26, apartado 8, del presente Reglamento, cuando proceda.

ANEXO IX

Información que debe presentarse para la inscripción en el registro de los sistemas de IA de alto riesgo enumerados en el anexo III en relación con las pruebas en condiciones reales de conformidad con el artículo 60

Con respecto a las pruebas en condiciones reales que vayan a inscribirse en el registro de conformidad con el artículo 60, se facilitará y se actualizará debidamente la información siguiente:

1. El número de identificación único para toda la Unión de la prueba en condiciones reales.
2. El nombre y los datos de contacto del proveedor o proveedor potencial y de los responsables del despliegue que participen en la prueba en condiciones reales.
3. Una breve descripción del sistema de IA, su finalidad prevista y demás información necesaria para la identificación del sistema.
4. Un resumen de las principales características del plan de la prueba en condiciones reales.
5. Información sobre la suspensión o la conclusión de la prueba en condiciones reales.

ANEXO X

Actos legislativos de la Unión relativos a sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia

1. Sistema de Información de Schengen

a) Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular (DO L 312 de 7.12.2018, p. 1).

b) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L 312 de 7.12.2018, p. 14).

c) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

2. Sistema de Información de Visados

a) Reglamento (UE) 2021/1133 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (UE) n.º 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 y (UE) 2019/818 en lo que respecta al establecimiento de las condiciones para acceder a otros sistemas de información de la UE a efectos del Sistema de Información de Visados (DO L 248 de 13.7.2021, p. 1).

b) Reglamento (UE) 2021/1134 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (CE) n.º 767/2008, (CE) n.º 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 y (UE) 2019/1896 del Parlamento Europeo y del Consejo y por el que se derogan las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, a fin de reformar el Sistema de Información de Visados (DO L 248 de 13.7.2021, p. 11).

3. Eurodac

a) Reglamento (UE) 2024/1358 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la creación del sistema «Eurodac» para la comparación de datos biométricos a efectos de la aplicación efectiva de los Reglamentos (UE) 2024/1315y (UE) 2024/1350 del Parlamento Europeo y del Consejo y de la Directiva 2001/55/CE del Consejo y de la identificación de nacionales de terceros países y apátridas en situación irregular, y sobre las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de garantía de cumplimiento del Derecho, por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) 2019/818 del Parlamento Europeo y del Consejo y se deroga el Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo (DO L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Sistema de Entradas y Salidas

a) Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011 (DO L 327 de 9.12.2017, p. 20).

5. Sistema Europeo de Información y Autorización de Viajes

a) Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226 (DO L 236 de 19.9.2018, p. 1).

b) Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV) (DO L 236 de 19.9.2018, p. 72).

6. Sistema Europeo de Información de Antecedentes Penales en relación con los nacionales de terceros países y apátridas

   Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

7. Interoperabilidad

   a) Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo (DO L 135 de 22.5.2019, p. 27).

   b) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

ANEXO XI

Documentación técnica a que se refiere el artículo 53, apartado 1, letra a) — documentación técnica para proveedores de modelos de IA de uso general

Sección 1

Información que deben presentar los proveedores de modelos de IA de uso general

La documentación técnica a que se refiere el artículo 53, apartado 1, letra a), incluirá como mínimo la siguiente información en función del tamaño y perfil de riesgo del modelo:

1. Una descripción general del modelo de IA de uso general que incluya:

   a) las tareas que el modelo vaya a realizar y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;

   b) las políticas de usos aceptables aplicables;

   c) la fecha de lanzamiento y los métodos de distribución;

   d) la arquitectura y el número de parámetros;

   e) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;

   f) la licencia.

2. Una descripción detallada de los elementos del modelo a que se refiere el punto 1 e información pertinente sobre el proceso de desarrollo que incluya los siguientes elementos:

   a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para integrar el modelo de IA de uso general en los sistemas de IA;

   b) las especificaciones de diseño del modelo y el proceso de entrenamiento, incluidos los métodos y las técnicas de entrenamiento, las decisiones clave de diseño, incluidas la justificación lógica y los supuestos de los que se ha partido; aquello que el modelo está diseñado para optimizar y la pertinencia de los diversos parámetros, según proceda;

   c) información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión (por ejemplo, limpieza, filtrado, etc.), el número de puntos de datos, su alcance y sus principales características; cómo se obtuvieron y seleccionaron los datos, así como cualquier otra medida que permita detectar que las fuentes de datos no son idóneas y los métodos para detectar sesgos identificables, cuando proceda;

   d) los recursos computacionales utilizados para entrenar el modelo (por ejemplo, número de operaciones de coma flotante, el tiempo de entrenamiento y otros detalles pertinentes relacionados con el mismo;

   e) el consumo de energía conocido o estimado del modelo.

   A propósito de la letra e), cuando se desconozca el consumo de energía del modelo, podrá hacerse una estimación del consumo de energía a partir de la información relativa a los recursos computacionales utilizados.

Sección 2

Información adicional que deben presentar los proveedores de modelos de IA de uso general con riesgo sistémico

1. Una descripción detallada de las estrategias de evaluación, con los resultados de la misma, sobre la base de los protocolos y herramientas de evaluación públicos disponibles o de otros métodos de evaluación. Las estrategias de evaluación incluirán los criterios de evaluación, los parámetros y el método de detección de limitaciones.

2. Cuando proceda, una descripción detallada de las medidas adoptadas para realizar pruebas adversarias internas o externas (por ejemplo, utilización de «equipos rojos») y adaptaciones de los modelos, incluida su alineación y puesta a punto.

3. Cuando proceda, una descripción detallada de la arquitectura del sistema, con una explicación de la manera en que se incorporan o enriquecen mutuamente los componentes del software y de la manera en que se integran en el procesamiento general.

ANEXO XII

Información sobre transparencia a que se refiere el artículo 53, apartado 1, letra b) — documentación técnica de los proveedores de modelos de IA de uso general para los proveedores posteriores que integren el modelo en su sistema de IA

La información a que se refiere el artículo 53, apartado 1, letra b), incluirá como mínimo la siguiente información:

1. Una descripción general del modelo de IA de uso general que incluya:
   a) las tareas que el modelo vaya a realizar y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;
   b) las políticas de usos aceptables aplicables;
   c) la fecha de lanzamiento y los métodos de distribución;
   d) la manera en que el modelo interactúa o puede utilizarse para interactuar con el *hardware* o el software que no formen parte del propio modelo, cuando proceda;
   e) las versiones del software pertinente relacionadas con el uso del modelo de IA de uso general, cuando proceda;
   f) la arquitectura y el número de parámetros;
   g) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;
   h) la licencia del modelo.
2. Una descripción de los elementos del modelo y de su proceso de desarrollo, incluidos:
   a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para integrar el modelo de IA de uso general en los sistemas de IA;
   b) la modalidad (por ejemplo, texto, imagen, etc.) y el formato de las entradas y salidas y su tamaño máximo (por ejemplo, longitud de la ventana de contexto, etc.);
   c) información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión.

ANEXO XIII

Criterios para la clasificación de los modelos de IA de uso general con riesgo sistémico a que se refiere el artículo 51

Con el fin de determinar si un modelo de IA de uso general tiene unas capacidades o unos efectos equivalentes a los contemplados en el artículo 51, apartado 1, letra a), la Comisión tendrá en cuenta los siguientes criterios:

a) el número de parámetros del modelo;

b) la calidad o el tamaño del conjunto de datos, por ejemplo medidos a través de criptofichas;

c) la cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo;

d) las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas);

e) los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso;

f) si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la Unión;

g) el número de usuarios finales registrados.