Capítulo 1.
La inteligencia artificial y responsabilidad civil: situación actual y perspectiva de futuro

Ana Isabel Berrocal Lanzarot

Profesora Contratada Doctora de Derecho Civil (acreditada a profesor Titular)
Universidad Complutense de Madrid

1. CONSIDERACIONES PREVIAS

La inteligencia artificial 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 inteligencia artificial puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de la asistencia sanitaria, la agricultura, la 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[1], la eficiencia de los recur-

1 En la entrevista a María José Rivas y Alfonso Peralta Gutiérrez, directores de las Jornadas Internacionales "Desafíos jurídicos de la IA" indican que la IA va a llegar a los tribunales no sólo con automatización de procesos o uso de la IA generativa, sino también en la función jurisdiccional (Diario La Ley, de 6 de septiembre de 2024, p. 1.

Por su parte, DELGADO MARTÍN, J. (2024). "Notas sobre el uso de la IA generativa por profesionales del sistema de justicia", *Diario La Ley, nº 10568, Sección Tribuna, de 16 de septiembre*, p. 2 manifiesta, al respecto, que "el uso de instrumentos de IA generativa en la justicia tiene riesgos de imprecisión, es decir, de producir resultados inexactos, incompletos, engañosos o desactualizados. Téngase en cuenta que la salid que generan los chatbots de IA es lo que el modelo predice como la combinación de apalabras más probables, basada en los documentos y datos que tiene como información fuente. Téngase en cuenta que, por la forma de funcionamiento de estos sistemas IA, no siempre la siguiente palabra más probables es la más correcta o adecuado desde el punto de vista fáctico y/o jurídico. De esta manera, el sistema de IA puede aportar sentencias ficticias; referirse a legislación, artículos o textos legales que no existen; o puede inventarse citas o referencias". Y añade que "este tipo de IA puede resultar útil para hallar material ya conocido como correcto, pero que no se encuentra fácilmente disponible; para realizar una primera aproximación., pero siempre que después el resultado sea confirmado con fuentes fiables (…). Sin embargo, su utilización no resulta aconsejable para realizar investigaciones con la finalidad de encontrar nueva información legal que no se puede verificar".

sos 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.

Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concreto, 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.

Por otra parte, los sistemas de Inteligencia Artificial (IA) pueden desplegarse con facilidad en la sociedad, también a escala transfronteriza, y circular fácilmente por toda la Unión. Algunos Estados miembros ya han estudiado la 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. Ello conlleva la existencia de normas nacionales divergentes y, asimismo, 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 vienen a obstaculizar la libre circulación, la innovación, el despliegue y la adopción en el mercado interior de los sistemas de IA y los productos y servicios conexos mediante el establecimiento de obligaciones uniformes para los operadores y la garantía de una protección igual 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 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 se han de establecer normas que regulen la introducción en el mercado, la puesta en servicio y la utilización de determinados sistemas de IA, lo que garantiza el buen funcionamiento del mercado interior y permite 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.

De ahí, la necesidad imperiosa de la aprobación del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, de Inteligencia artificial (en adelante, RIA) que, precisamente, es fruto de largas negociaciones en el seno de las instituciones europeas y nace en el contexto de la Estrategia Europea de Inteligencia Artificial de la Comisión Europea, a través de la cual se pretende convertir a la Unión Europea en una región de referencia mundial para la Inteligencia Artificial, garantizando el respeto a los derechos fundamentales, la democracia, el Estado de Derecho y la sostenibilidad medio ambiental[2]. Al mismo tiempo, el Reglamento IA tiene por objetivo impulsar la innovación y posicionar a la Unión Europea como líder en el campo de la Inteligencia artificial y de la industria. Lo que, puede influir en otras legislaciones extranjeras por el llamado "efectos Bruselas".

La RIA regula la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión Europea. Su principal objetivo es fomentar el desarrollo y la utilización de la IA en el seno de ese ámbito geográfico, así como garantizar un alto nivel de protección de la salud, la seguridad y los derechos fundamentales, poder contribuir al 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 y garantizar la protección de los principios ético, como solicitó específicamente el Parlamento Europeo[3].

---

2 Respecto a su entrada en vigor y aplicación el artículo 113 de este Reglamento dispone, al respecto, que entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea y, será aplicable a partir del 2 de agosto de 2026. No obstante: a) Los capítulos I. Disposiciones Generales y II, Sistemas prohibido serán aplicables a partir del 2 de febrero de 2025; b) El capítulo III. Sistemas de IA de alto riego; sección 4ª. Autoridades notificantes y organismo notificado; el capítulo V. Modelos de IA de uso general; el capítulo VII. Gobernanza; y el capítulo XII. Sanciones y el artículo 78. Confidencialidad serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101. Multas a proveedores de modelo de IA de uso general; c) El artículo 6, apartado 1. Reglas de clasificación de los sistemas de IA de alto riesgo y obligaciones derivadas y las obligaciones correspondientes de este Reglamento serán aplicables a partir del 2 de agosto de 2027. Si bien, este Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

De todas formas, entre las obligaciones de evaluación y revisión destacar que 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 de este Reglamentos 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 (artículo 112.1). por otra parte, a más tardar el 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión evaluará: 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; y, c) La necesidad de mejorar la eficacia del sistema de supervisión y gobernanza (artículo 112.2).

3 Para BARRIO ANDRÉS, M. (2024). "Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial", *Diario La Ley, núm. 86, sección ciberderecho, de 30 de julio*, pp. 2 y 3 "El Reglamento es técnicamente una norma muy compleja. Su proceso normativo de elaboración, especialmente en su fase final, ha dejado mucho que desear. La influencia de ciertos grupo ha sido innegable y ha tenido su reflejo, por ejemplo, en una regulación sui generis de la IA generativa"; y, añade se trata "en suma de una norma muy enrevesada y con evidentes problemas de calidad normativas". Por lo que a juicio del autor, estas críticas están justificadas. No obstante, señala que "no deben olvidarse los numerosos beneficios que

En este contexto, la RIA garantiza la libre circulación transfronteriza de mercancías y servicios basados en la IA, con lo que impide que los Estados miembros puede imponer restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que este Reglamento lo autorice expresamente.

Ahora bien, 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. 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.

Sobre tales bases, el RIA busca promover la adopción de una IA fiable y centrada en el ser humano y asegurar un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales frente a los riesgos potenciales de la IA.

Por otra parte, 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 definidos, 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.

Si bien, este 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[4].

---

la legislación recién aprobada pretende aportar para la integración europea. La seguridad de cara al futuro consiste en una legislación que sea eficaz y se adapte a pesar de los cambios jurídicos, sociales y técnicos que se produzca con el tiempo".

4 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

Sin perjuicio de los requisitos jurídicamente vinculantes del RIA 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. Efectivamente, como señala, al respecto, el considerando 2 del RIA "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"; y reitera el considerando 6 del citado Reglamento: "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, los derechos y libertades fundamentales consagrados en los Tratados y, de conformidad con el artículo 6 del TUE. 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".

En este contexto, un enfoque basado en el riesgo conlleva definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes que participen en la cadena de valor. Las obligaciones no se limitan a los proveedores de sistemas de IA, sino que alcanzan también entre otros, a quienes utilizan sistemas de IA para fines profesionales, que reciben el nombre de responsables del repliegue.

Asimismo, resulta necesario prohibir determinadas prácticas de IA que no son aceptables, así como imponer obligaciones de transparencia a determinados sistemas de IA. Además, se cataloga ciertos sistemas de IA como de alto riesgo y se establecen exigentes requisitos para estos sistemas, así como obligaciones para los participantes en la cadena de valor, incluidas las empresas que utilicen sistemas de IA. Estos sistemas de alto riesgo se dividen en dos grandes grupos: por un lado, mediante un análisis del riesgo se han identificado un conjunto de familias de sistema de IA que, puede considerarse de alto riesgo, si su salida es relevante

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.

respecto a una acción, o decisión que puede presentar un riesgo a la salud, seguridad o los derechos fundamentales. De ahí que, el RIA enumere y describa este conjunto, en el que se incluye entre otros sistemas de identificación biométrica, de protección de las infraestructuras críticas, de selección y promoción personal, de utilización en fronteras, o los usados por las Fuerzas y Cuerpos de Seguridad del Estado o la Administración de Justicia. Si bien, la Comisión puede actualizar esta lista mediante un acto delegado; por otro lado, existen productos que ya están regulados por normativa armonizada de la UE y que bajo esta normativa están sujetos a evaluación de conformidad. Así, un sistema de IA que constituya uno de estos productos o puede constituir un componente de seguridad de uno de los mismo se sujetarán a su correspondiente normativa armonizada.

De ahí, la conveniencia de 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.

En este contexto, también, se regula la introducción en el mercado de modelos de IA de uso general. Igualmente, se impone obligaciones de transparencia en relación con determinados sistemas de IA especialmente los destinados a interactuar con personas físicas y a la generación de contenidos.

Por otra parte, el RIA define varias entidades de supervisión: existirá al menos una autoridad nacional notificante y una autoridad de supervisión de mercado como autoridades nacionales competentes para lograr aplicar los propósitos del Reglamento[5]. Las autoridades de supervisión del mercado procederán a monotorizar el correcto funcionamiento, ya en el mercado, de sistemas de IA de

5 En España, la autoridad de vigilancia del mercado competente es la Agencia Española de Supervisión de la IA (AESIA). Se trata de un ente con personalidad jurídica pública, con patrimonio propio y autonomía en su gestión y potestad administrativa. Actuará con independencia orgánica y funcional de las Administraciones Públicas y de forma objetiva y transparente e imparcial, llevando a cabo medidas destinadas a la minimización de riesgos significativos por el uso de sistemas de Inteligencia Artificial sobre la seguridad y la salud de las personas, así como sobre los derechos fundamentales. Está adscrita al Ministerio para la Transformación Digital y de la Función Público, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Tiene sede en A Coruña. AESIA cuenta con una dotación presupuestaria de 5 millones de euros.

La Ley 22/2021, de 28 de diciembre de Presupuestos Generales del Estado para 2022 recoge en su Disposición Adicional centésimo trigésima la creación precisamente, de la Agencia Española de Supervisión de IA. También la Ley 28/2022, de 21 de diciembre de fomento de ecosistemas de las empresas emergentes, conocida como Ley *startups*, prevé la creación de la AESIA. Por otra parte, AESIA se regirá por su Estatuto aprobado mediante el Real Decreto 729/2023, de 22 de agosto por el que se aprueba el Estatuto de AESI (BOE, núm. 201, 2 de septiembre de 2023, pp. 122289 a 122316); y, por la Ley 40/2015, de 1 de octubre del Régimen Jurídico del Sector Publico.

alto riesgo, identificando riesgos sobrevenidos, incidentes u otras situaciones que exijan tomar medidas sobre los sistemas de IA de alto riesgo. En el esquema de certificación de productos que propone el RIA, una autoridad notificante podrá habilitar a organismos de evaluación de conformidad parta hacer las evaluaciones de conformidad en materia de IA a productos que quieran comercializar o poner en funcionamiento los proveedores. Los sistemas de IA regulados por su propia normativa estarán supervisados por la autoridad de supervisión designada en dicha normativa. Para el caso de sistemas de identificación biométrica utilizados para fuerzas y cuerpos de seguridad del estado, migración y administración de justifica, las autoridades de supervisión serán o bien las autoridades nacionales de supervisión de las actividades de seguridad, migración y asilo, o bien la Agencia Española de Protección de Datos.

A nivel europeo, se constituirá un Consejo Europeo de Inteligencia Artificial donde participará un representante de cada Estado miembros[6]. El Consejo orientará sobre la implementación de la RIA, elaborará guías y establecerá reglas básicas para elaborar sandboxes[7]. De esta forma, contribuye un sistema institucional de gobernanza y supervisión y prevé elevadas sanciones y multas por infracciones del Reglamento.

Este RIA se complementa con otras iniciativas legislativas, en particular dos propuestas de Directivas que se hallan actualmente en tramitación. Por una parte, la Propuesta de Directiva sobre responsabilidad civil en materia de IA que, establece normas procesales sobre prueba en relación con procedimientos de responsabilidad civil extracontractual por daños y perjuicios que causen daños o pérdidas de datos, posibilitando reclamar una indemnización al proveedor de sistemas de IA o a cualquier fabricante que integre un sistema de IA en otro producto; y, por otra, con la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, ambas de 28 de septiembre de 2022 que, tiene por objeto: "establecer normas comunes sobre la responsabilidad de los operadores económicos por los daños sufridos por personas físicas causados por productos defectuosos" (artículo 1), definiéndose producto como "cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble; por "producto" se entiende también la electricidad, los archivos de fabricación digital y los programas informáticos (artículo 4.1) y considerándose producto defectuoso "cuando no ofrece la seguridad que el público en general tiene derecho a esperar, teniendo en cuenta todas las circuns-

6 El artículo 65 del RIA prevé la creación del Consejo Europeo de Inteligencia Artificial que, estará compuesto por un representante por cada Estado y, el artículo 66 del citado cuerpo legal se concretan sus funciones, entre otras, prestar asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del RIA.

7 España ha aprobado, al respecto, se ha aprobado el Real Decreto 817/2023, de 8 de noviembre que, establece un entorno controlado de pruebas para el ensayo de cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece normas armonizadas en materia de inteligencia artificial (BOE, núm. 268, de 9 de noviembre de 2023, pp. 149138 a 149168).

tancias, incluso: a) La presentación del producto, incluidas las instrucciones de instalación, uso y mantenimiento; b) El uso razonablemente previsible y el uso indebido del producto; c) El efecto en el producto de la posibilidad de seguir aprendiendo después del despliegue; d) El efecto sobre el producto de otros productos que quepa esperar razonablemente que se utilicen junto con el producto; e) El momento en que el producto fue introducido en el mercado o puesto en servicio o, si el fabricante conserva el control sobre el producto después de ese momento, el momento en que el producto dejó el control del fabricante; f) Los requisitos de seguridad del producto, incluidos los requisitos de ciberseguridad pertinentes para la seguridad; g) Cualquier intervención de una autoridad reguladora o de un operador económico contemplado en el artículo 7 en relación con la seguridad de los productos; h) Las expectativas específicas de los usuarios finales a los que se destina el producto. Si bien, no se considera defectuosos un producto por la única razón de que ya se haya introducido en el mercado o puesto en servicio, o se introduzca en el mercado o se ponga en servicio posteriormente, un producto mejor, incluidas las actualizaciones o mejoras de un producto (artículo 6).

Por lo demás, el RIA se entiende 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; en particular, el RIA no afecta a las obligaciones que impone el Reglamento General de Protección de Datos a los proveedores y responsables del despliegue en su papel de responsables o encargados del tratamiento, cuando el desarrollo o la utilización de los sistemas de IA impliquen el tratamiento de datos personales.

El derecho fundamental a la protección de los datos personales está garantizado por los Reglamentos (UE) 2016/679 y (UE) 2018/1725 del Parlamento Europeo y del Consejo y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. Además, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo 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 RIA 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 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 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. Ciertamente, 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. En todo caso, 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.

Por otra parte, el RIA debe interpretarse sin perjuicio de las disposiciones del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo relativas a la responsabilidad de los prestadores de servicios intermediarios.

Pues bien, el texto del RIA es extenso y complejo. Así se estructura en un total de 180 Considerandos, 113 artículos y 13 anexos con la asignación de contenidos materiales en Capítulos (un total de 13). Si bien, en algunos puntos deberá ser desarrollado y aclarado mediante disposiciones y directrices de la Comisión Europea.

Sobre tales bases, debe definirse con claridad el concepto de "sistema de IA" 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 posibilita 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 *softwar*e 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.

Asimismo, debe hacerse referencia a 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, así se aprende 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" alude 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 este 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) (considerando núm. 12 del RIA).

Por lo que, atendiendo a lo expuesto, se entenderá por "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. Esta definición se corresponde con la proporcionada por la OCDE (2019, revisado en 2023), que la RIA adopta con el objetivo de facilitar la convergencia de nociones a escala internacional. Quedan fuera de la misma y, por tanto, de la regulación, los sistemas de *software* de capacidades inferiores a las indicadas"[8]. Y por "riesgo" se considera: la combinación de la probabilidad de

8 Para BARRIO ANDRÉS, M. (2024). "Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia artificial". En: M. Barrio Andrés (dir), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch, pp. 35-36 "la definición no pretende abarcar los sistemas de software o enfoques de programación tradicionales más sencillo y el RIA habilita a la Comisión para que elabore directiva sobre su aplicación que resultarán en este punto fundamentales". A lo que añade que "la definición positivizada en el RIA pretende reflejar el consenso científico que los objetivos de un sistema de IA pueden ser *explícitos*

que se produzca un perjuicio y la gravedad de dicho perjuicio (artículo 2.1 y 2 de la RIA).

Ahora bien, 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. Como 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. Precisamente, la alfabetización en materia de IA deberá 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, podrán contribuir a mejorar las condiciones de trabajo y, en última instancia, sostener la consolidación y la innovación de una IA fiable en la Unión. Corresponde al Consejo Europeo de Inteligencia Artificial 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, asimismo, 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.

El artículo 4 del RIA dispone a tal efecto que *"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".*

(por ejemplo, cuando están directamente programados en el sistema por un desarrollador humano) o *implícitos*, o cuando el sistema es capaz de aprender nuevos objetivos)". Por su parte, MARTÍN CASALS, M. (2023). "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *Indret, núm. 3*, p. 61 señala que esta definición "(…) se quiere basar en características clave de la inteligencia artificial, como sus capacidades de aprendizaje, razonamiento o modelado, para distinguirla de sistemas de software o enfoques de programación más simples. Dado que los sistemas de IA están diseñados para operar con diferentes niveles de autonomía, la definición requiere que el sistema tenga al menos cierto grado de independencia de las acciones de los controles humanos y de las capacidad para operar sin intervención humana".

Además de la alfabetización resulta necesario el despliegue del sistema de IA a nivel educativo.

El presente estudio se va a centrar en el análisis de los sistemas de alto riesgo regulados en el RIA, específicamente, en los requisitos de tales sistemas, las obligaciones que asumen el proveedor, responsable del despliegue, importador, distribuidos y operador con la comercialización y puesta en servicio; y en la responsabilidad civil que se deriva de los daños que puedan causar en las personas, atendiendo a la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial de 28 de septiembre de 2022.

Por otra parte, antes de comenzar nuestro análisis de la materia, nos parece oportuno señalar que, el 17 de mayo de 2024 se celebró la 133ª sesión del Comité de Ministros del Consejo de Europa, donde ser aprobó el Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, tratándose del primer acuerdo internacional en este ámbito. Este Convenio ha sido elaborado por el Comité de Inteligencia, que reúne a los 46 Estados miembros del Consejo de Europa, además de 11 Estados no miembros (Argentina, Australia, Canadá, Costa Rica, Estados Unidos, Israel, Japón, México, Perú, la Santa Sede y Uruguay) y representantes del sector privado, la sociedad civil y el mundo académico, en calidad de observaciones. La Unión Europea ya ha autorizado la firma mediante la Decisión (EU) 2024/2218 del Consejo de 28 de agosto de 2024 relativa a la firma, en nombre de la Unión Europea, del Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho, publicada en el BOE de 4 de septiembre de 2024 y en el DOUE de 4 de septiembre de 2024. Este documento establece principios generales y obligaciones para las partes del convenio, asegurando que la implementación de sistemas de IA no comprometa los valores fundamentales de la sociedad y los proteja. Y, por supuesto, que las actividades concernientes con la seguridad nacional están excluidas del ámbito de aplicación del Convenio. El Convenio destaca la importancia de la IA ética y responsable que respete la privacidad individual y fomente una sociedad justa e inclusiva. Además, reconoce la necesidad de transparencia en los algoritmos de la IA y la rendición de cuentas de los desarrolladores y operadores de estos sistemas. Esta Decisión (UE) 2024/2218 es un reflejo de la voluntad política de la UE de liderar globalmente en la definición de los estándares ético para la IA, y de su deseo de colaborar con otros Estados miembros del Consejo de Europea para lograr este objetivo. Ciertamente, la citada Decisión (EU) 2024/2218 supone un paso adelante en la consolidación de un enfoque coherente y unificado hacia la IA en Europa, buscando garantizar su desarrollo se alinee con los valores y principios democrático. Este documento no sólo establece un marco legal para la IA, sino que también sirve como una declaración de los valores y aspiraciones de la UE en la era de la tecnología avanzada.

2. OBJETIVO Y ÁMBITO DE APLICACIÓN DEL RIA

Antes de referirnos a los aspectos jurídicos indicados procede señalar que, 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. 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. Este 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. Por otra parte, el RIA no debe afectar a las disposiciones destinadas a mejorar las condiciones laborales en el trabajo en plataformas digitales establecidas en la Directiva del Parlamento Europeo y del Consejo relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales. Además, 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 de este 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 de este Reglamento o persiga objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Así, este 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 nº 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.

Pues bien, en este contexto, el objetivo del RIA aparece concretado en su artículo 1, que se puede sintetizar en lo siguiente:

1. Mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme;
2. Promover la adopción de una inteligencia artificial 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 prestar apoyo a la innovación;
3. Establecer normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión;
4 Prohibir determinadas prácticas de IA;
5 Concretar los requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;
6. Disponer normas armonizadas de transparencia aplicables a determinados sistemas de IA; normas armonizadas para la introducción en el mercado de modelos de IA de uso general; y, normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento;
7. Establecer medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.

Asimismo, precisa el considerando núm. 1 del RIA: "el objetivo de este 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 la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial 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, 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".

En cuanto su ámbito de aplicación, marcado por el principio de la extraterritorialidad precisa el considerando núm. 21 del RIA que "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 este Re-

glamento 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".

Desde un punto de vista subjetivo se aplica 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. El artículo 3.3 de la RIA define proveedor como: 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;

b) Los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión. El artículo 3.4 de la RIA los conceptúa como: 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;

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. Si bien, añade el considerando núm. 22 del RIA: "(…) 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;

d) Los importadores y distribuidores de sistemas de IA. El artículo 3.6 y 7 del RIA los define: los primeros como: 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 y al distribuido como: 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;

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. Se entiende por 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; y, "puesta en servicio" como: 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 (artículo 3.9 y 10 del RIA);

f) Los representantes autorizados de los proveedores que no estén establecidos en la Unión. Los conceptúa el artículo 3.5 del RIA como: 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;

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

Asimismo, se define *operador* en el artículo 3.8 como: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor.

En todo caso, como precisa el RIA sus normas armonizadas también deben aplicarse a las instituciones, órganos y organismos de la Unión cuando actúen como proveedores o responsables del despliegue de un sistema de IA (considerando núm. 22).

Desde un punto de vista objetivo, puede señalarse que en el RIA se contienen una serie de excepciones materiales relativas a su aplicación. Así se *excluye* del ámbito del Reglamento:

1. Los sistemas de IA que 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. 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, siendo éste 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 este 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 de este Reglamento y los proveedores de dichos sistemas deben garantizar el cumplimiento de este 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 de este 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 de este Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades (considerando núm. 24 del RIA);

2. 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;
3. Tampoco se aplicará a las autoridades públicas de terceros países, ni a las organizaciones internacionales, 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; igualmente, 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. En fin, 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 esta exclusión;
4. Tampoco 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 (utilicen los sistemas de IA con fines puramente personales);
5. Con el objetivo de apoyar la innovación, respetar la libertad de ciencia y no socavar la actividad de investigación y desarrollo es necesario también excluir del ámbito de aplicación del Reglamento 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 este 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. Respecto a la actividad de investigación, prueba y desarrollo orientada a productos en relación con sistemas o modelos de IA tampoco deben aplicarse las normas de este Reglamento 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 con lo dispuesto en

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 mismo, así como de la aplicación de disposiciones sobre espacios controlados de pruebas para la IA y pruebas en condiciones reales. En todo caso, 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 de este Reglamento. De todas formas, 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 (considerando núm. 25 del RIA);

6. 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 del RIA.

Ciertamente, la Unión Europea pretende centrar el esfuerzo normativo en aquellos usos y sistemas de IA que generen un riesgo relevante en el mercado de la Unión Europea, con el fin de no obstaculizar el desarrollo de la IA o actividades de investigación y otros ámbitos con poco impacto como el uso doméstico.

En este contexto, como hemos indicado, este 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; asimismo, 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; ni 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. Por otra parte, 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; y, en fin, ni la aplicación del Derecho de la Unión Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones respecto a los datos personales tratados en relación con los derechos y obligaciones establecidos en el RIA.

Sobre tales bases, los principales sujetos contemplados en el RIA son los siguientes:

* Proveedor: 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 ge-

neral y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente. Conviene precisar que, una persona física o jurídica concreta, definida como el proveedor debe asumir la responsabilidad asociada a la introducción en el mercado o la puesta en servicio de un sistema de IA de alto riesgo; todo ello, con independencia de si dicha persona física o jurídica es o no quien diseñó o desarrolló el sistema.

* Importador: 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.
* Distribuidor: 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.
* Responsable del despliegue: 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. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del responsable del despliegue.
* También se hace referencia al "proveedor posterior" como: 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 3.68 del RIA).

En todo caso 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. 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, además, 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 RIA. Cuando resulte

procedente, 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. En todo caso, 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 proveedores que sean pymes, incluidas las empresas emergentes, cuando establezcan las tasas aplicables a las evaluaciones de la conformidad. Por su parte, 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. Así, 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.

Con el fin, precisamente, de abordar las necesidades específicas de las pymes, incluidas las empresas emergentes, la Comisión debe proporcionar modelos normalizados para los ámbitos regulados por este 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 contenido de este 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 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 de este Reglamento.

Bajo el parámetro 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 RIA, 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 aplica-

ción 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, especialmente, capaces de proporcionar a los proveedores y organismos notificados asistencia técnica y científica dentro de sus respectivas misiones y esferas de competencia.

Si bien, 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 con una de las obligaciones más costosas, en concreto, la de establecer un sistema de gestión de la calidad y que la haga 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.

De ahí que, resulte 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.

En todo caso, todos los Estados miembros y, por ende, los sujetos reseñados 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 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.

Igualmente, con respecto a los menores procede señalar que, 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 ya citada Observación General nº 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. De forma que, cuando se evalúe la gravedad del perjuicio que puede ocasionar un sistema de IA, se tendrá presente la situación de vulnerabilidad de los menores.

En este contexto, procede indica que, desde un ámbito territorial: Con relación a la aplicación del RIA a Reino Unido, Irlanda y Dinamarca los considerandos núm. 40 y 41 disponen respectivamente que: "De conformidad con el artículo 6 bis del Protocolo nº 21 sobre la Posición del Reino Unido y de Irlanda respecto del Espacio de Libertad, Seguridad y Justicia, anejo al TUE y al TFUE, 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". Y, "de conformidad con lo dispuesto en los artículos 2 y 2 bis del Protocolo nº 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".

3. CLASIFICACIÓN Y GESTIÓN DE LOS SISTEMAS DE RIESGOS

El RIA estudia la inteligencia artificial desde los riesgos que pueden entrañar a las personas y procura adaptar el tipo y contenido de las obligaciones de conformidad con el alcance y la gravedad de los riesgos que pueda suponer. Ciertamente, 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 generan unos riesgos aceptables; concretar 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[9]. Se opta por un enfoque basado en el riesgo, mediante técnicas de *Compliance*, concretando los siguientes sistemas[10]:

1. Sistemas de riesgo inaceptable para la Unión Europea: el RIA prohíbe determinadas prácticas de IA por entender que representan un riesgo inaceptable por afectar a la salud, derechos fundamentales. En concreto, el RIA prohíbe las siguientes prácticas: a) El empleo de técnicas subliminales, manipuladoras y engañosas: se trata de 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[11]; b) Explotación de vulnerabilidades

9 Vid., MARTÍN CASALS, M. (2023). "La propuesta de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *op. cit.,* p. 63.

10 Un análisis de la clasificación y gestión de riesgos previsto en el RIA, vid., CAMPOS ACUÑA, C. (2024). "Las 15 claves del Reglamento Europeo de Inteligencia Artificial (AI Act) (1)", *El Consultor de los Ayuntamientos, de 15 de julio*, pp. 3-5.

11 El considerando núm. 28 del RIA dispone que: "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". Y, añade el considerando núm. 29 del RIA que: "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

de una persona o de un colectivo: supone 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) Los sistemas para evaluar o clasificar a las personas físicas o colectivos durante un periodo de tiempo atendiendo a su comportamiento social o características (*sistemas que permite un social scoring por parte de los gobiernos y autoridades públicas*): 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

---

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 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 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, 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".

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) Los sistemas para valorar o predecir el riesgo que una persona física cometa un delito: 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 creación o ampliación de bases de datos de reconocimiento facial masivo: 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) Los sistemas de IA para inferir emociones de una persona física en centros de trabajo o educativos: 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[12]; g) Categorización biométrica para inferir datos de categorías especiales: 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. Como precisa el considerando núm. 30 del RIA *"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*

12 El considerando núm. 18 del RIA relativo al concepto de "sistema de reconocimiento de emociones" 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".

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"[13]; h) Identificación biométrica remota en tiempo real en lugares públicos con fines policiales: 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[14].

Ahora bien, conviene precisar que 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 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 po-

13 Por su parte, en el considerando núm. 16 del RIA se refiere al concepto de "categorización biométrica" y lo define 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".

14 Se trata de delitos de 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 y tejidos humanos, entre otros.

sible 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, 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. Por otra parte, 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.

Sobre tales bases, 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 del artículo 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 mencionados, 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. En todo caso, 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.

De todas formas, 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 artículo 5 del RIA. 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 del citado artículo 5, así como a la supervisión y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos expuestos en líneas precedentes, y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii) del mencionado artículo 5 apartado 1 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.

Como precisa los considerandos núm. 32 y 33 del RIA: "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".

"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 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 privativa 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 II del presente Reglamento se basa en los treinta y dos delitos enumerados en la Decisión Marco 2002/584/JAI del Consejo, 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, 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. Y añaden, al respecto, los considerandos número 34 y 35 del RIA que: "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". Y, "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 del Parlamento Europeo y del Consejo de 27 de abril de 2016. 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".

En todo caso, las normas del RIA, basadas en el artículo 16 del TFUE, que prohíben, con algunas excepciones, 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 (el tratamiento de datos biométricos) 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 este Reglamento, sin que haya margen, fuera del mismo, 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, este 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.

Si bien, 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 este 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 prevista en este Reglamento, ni a las normas de desarrollo aplicables del Derecho nacional que puedan hacer efectiva dicha autorización.

En fin, 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 presentarán a la Comisión informes anuales sobre dicho uso. Para ello, 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.

Por otra parte, 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.

En fin, también deben estar prohibidas 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, 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.

No obstante, lo expuesto las prohibiciones aplicables en el artículo 5 de la RIA se entiende sin perjuicio de lo que establezcan otras disposiciones de Derecho de la Unión.

Al respecto, precisa MARTÍN CASALS que "algunas de esas prohibiciones no son absolutas y están sujetas a excepciones en función del interés terapéutico de la medida con requerimiento de información necesaria a los afectados y, en su caso, previo consentimiento informado, como ocurre en el caso de la utilización de técnicas subliminales y de categorización biométrica"[15].

2. Sistemas de IA de alto riesgo. Se trata de sistemas de IA que pueden tener efectos relevantes y perjudiciales para la salud, la seguridad y, los derechos fundamentales de las personas. Están sujetos a una serie de requisitos y obligaciones de imperativo cumplimiento para poder acceder al mercado de la Unión Europea.

El Reglamento en su artículo 6 considera un sistema de IA de alto riesgo con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos, cuando reúna las dos condiciones siguientes:

a) Que el sistema de IA esté destinado a ser utilizado como componente de seguridad en determinados productos regulados; o el propio sistema de IA sea uno de dichos productos (por ejemplo, aviones, automóviles, juguetes, productos sanitarios) tal y como se identifican en el Anexo I del RIA.

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.

Además, de estas categorías se considera también sistemas de alto riesgo aquellos identificados de especial relevancia o sensibles en el Anexo III del RIA que, incluyen determinados usos de la IA en ámbitos como sistemas de identificación biométrica remota; infraestructuras críticas; educación y la formación profesional; empleo, gestión de trabajadores y acceso al autoempleo; acceso a los servicios privados esenciales y prestaciones públicas esenciales y el disfrute de estos servicios y prestaciones (por ejemplo, la sanidad o la banca) (sistemas desinados a ser utilizados para evaluar la solvencia de personas físicas o establecer si calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes

15 MARTÍN CASALS, M. (2023). "La propuesta de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *op. cit.*, p. 64.

financieros); determinados sistemas de las fuerzas de seguridad, 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; la Administración de justicia y los procesos democráticas (como influir en las elecciones).

Ahora bien, se deben 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. Por otra parte, 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.

Por otra parte, cuando se introduce en el mercado de la Unión, se pone al servicio o se utilizan sistemas de IA de alto riesgo su operatividad debe supeditarse al cumplimiento 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 van a plantear riesgos inaceptables para intereses públicos importantes de la Unión, reconocidos y protegidos por el Derecho de la Unión. Así, 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" la norma general es que más de un acto jurídico de la legislación de armonización de la Unión, como los Reglamentos (UE) 2017/745 y (UE) 2017/746 del Parlamento Europeo y del Consejo o la Directiva 2006/42/CE del Parlamento Europeo y del Consejo 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. De ahí que, para 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 de este Reglamento y de la legislación de armonización de la Unión incluida en una lista del Anexo I de este 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.

En este contexto, 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) nº 300/2008 del Parlamento Europeo y del Consejo, el Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo, el Reglamento (UE) nº 168/2013 del Parlamento Europeo y del Consejo, la Directiva 2014/90/UE del Parlamento Europeo y del Consejo, la Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, 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 este 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.

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 Anexo I de este Reglamento, procede clasificarlos como de alto riesgo en virtud del mismo 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, equipos 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.

Ahora bien, que un sistema de IA se clasifique como de alto riesgo en virtud de este 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.

En lo referente a los sistemas de IA independientes, esto es, 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 y de innovación, así como los posibles cambios en el uso de los sistemas de IA.

Por otra parte, 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.

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 mantener en el tiempo 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.

Asimismo, 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.

Ahora bien, sin perjuicio de las normas previstas en el Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, 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.

Sobre tales bases, conviene precisar que, el hecho que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud de este 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 (patente de corso) para el tratamiento de datos personales, incluidas las categorías especiales de datos personales, en su caso, salvo que este Reglamento disponga específicamente otra cosa.

En este contexto y 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 de este Reglamento deben tener en cuenta el estado actual de la técnica generalmente reconocida en materia de IA, ser proporcionadas y eficaces para alcanzar los objetivos de este Reglamento. Sobre la base del nuevo marco legislativo, como se aclara en la citada Comunicación de la Comisión titulada "Guía azul" sobre la aplicación de la normativa europea relativa a los productos de 2022" tratada en líneas precedentes, la norma general supone que más de un acto jurídico de la legislación de armonización de la Unión resulta 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 de este Reglamento se refieren a aspectos diferentes de los contemplados en la legislación de armonización de la Unión existente y, por consiguiente, los requisitos de este 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 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. De ahí que, para 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 el anexo III de este 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 de este Reglamento, en la documentación y los procedimientos ya existentes, exigidos por los actos legislativos de armonización de la Unión vigentes, basados, precisamente, en el nuevo marco legislativo y enumerados en el Anexo I de este Reglamento. Esto no debe socavar en modo alguno la obligación del proveedor de cumplir todos los requisitos aplicables.

A tal fin, 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 a este 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 adicio-

nales para mitigar los usos indebidos razonablemente previsibles, cuando resulte necesario y oportuno.

Por otra parte, 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. Y, resulta 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. Además, 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. Todo ello con el 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.

En todo caso, 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. En este ámbito de actuación, 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.

Ahora bien, 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 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. Además, 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, atendiendo a su finalidad y con arreglo al estado actual de la técnica generalmente reconocido.

Sobre tales bases, por un lado, procede desarrollar la necesaria solidez técnica y la ciberseguridad. En cuanto a 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. Y, con respecto a la ciberseguridad resulta es fundamental para garantizar que los siste-

mas 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.

Y, por otro, señalar que, frente a la opacidad y complejidad de determinados sistemas de IA y con el objetivo de 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. 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, además, 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.

3. Sistemas de IA de riesgo limitado. Son los supuestos contenidos en el artículo 50 del RIA. Así: Los sistemas de IA destinados a interactuar directamente con personas físicas. A tal fin, se diseñan y desarrollan de tal forma que las personas físicas estén informadas por el proveedor o usuario de que están interactuando con un sistema de IA para que puedan tomar una decisión informada de continuar

o no. Suponen el uso de sistemas de IA como *chatbot* o robots conversacionales; 2. 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 que constituyen *deep fakes*. Los proveedores velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y, asimismo, porque sea posible detectar que han sido generados o manipulados de manera artificial; 3. Sistemas de reconocimiento de emociones o sistemas de categorización biométrica. Los responsables del despliegue deberán informar del funcionamiento de estos sistemas 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. Los proveedores también tendrán que asegurarse que el contenido generado por IA es identificable. De forma que, el texto generado por IA y publicado deberá etiquetarse como generado artificialmente, si se quiere informal al público sobre asuntos de interés general; y, 4. Los sistemas de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación. Los responsables del despliegue deberán hacer 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.

En los términos apuntados, estos sistemas están sujetos requisitos de información y transparencia. Ahora bien, la información se facilitará a las personas físicas 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.

Por otra parte, esta obligación de transparencia 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.

En este contexto, 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. Asimismo, 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; y, 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.

4. Sistemas de IA de riesgo mínimo. No están regulados específicamente ni tienen que cumplir determinados requisitos, ni dan lugar a la exigencia de obligaciones. No obstante, sobre la base de lo dispuesto en el artículo 95.1 del RIA de fomentar y facilitar la elaboración de Código de conducta destinados, precisamente, a fomentar la aplicación voluntaria de alguno o de todos los requisitos establecidos en el capítulo III, sección 2ª", teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos. Serían, por tanto, todas las demás categorías no contenidas en las anteriores expuestas. Se trata de aquellos supuestos en los que las personas pueden decidir de libre sobre su uso (filtros de spam o videojuegos) [16].

5. Modelos de IA de uso general. Además de sistemas de IA, el RIA contempla también determinados modelos de IA. Los modelos de IA se integran en sistemas, pero no constituyen en sí mimos un sistema.

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. Suelen estar integrados en los sistemas de IA y formar parte de dichos sistemas.

El artículo 3.63 del RIA define como: 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; "capacidades de gran impacto": capacidades

16 MUÑOZ GARCÍA, C. (2024). "Modelos de Inteligencia Artificial de uso general y sistemas de riesgo limitado y mínimo". En. M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia Artificial*, Valencia: tirant lo blanch p. 107 precisa, al respecto que "no hay obligaciones imperativas; si bien, el RIA propone que se fomente el uso de códigos de conducta y la transparencia para cualquier sistema. Ni ocupan ni preocupan al legislador europeo, por lo que, no están regulados en el Reglamento"; de ahí que, para la autora "todo parece indicar que se puede hacer un uso conforme se considere".

que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados.

Por otra parte, el RIA 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 este 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 RIA. 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 este Reglamento cuando, tras haber realizado dichas actividades, el modelo se introduzca en el mercado.

Ahora bien, 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.

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.

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.

Sobre tales bases, 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, la información sobre la ar-

quitectura del modelo y 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.

Ciertamente, 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.

Por otra parte, 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 requieren 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 que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor.

Por su parte, el RIA conceptúa los "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 (artículo 3.66 del RIA). Estos 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 especial 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 este 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 de lo dispuesto en este Reglamento, así como con las autoridades competentes establecidas en el mismo.

Ciertamente, 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 gran tamaño o en motores de búsqueda en línea también de 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 RIA, 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 y de motores de búsqueda ambas de 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.

Centrándonos, por razones de espacio, solo en los sistemas de IA de alto riesgo, procede referirse a continuación a los requisitos exigibles a estos sistemas y las obligaciones relativas a los sistemas de alto riesgo que asumen los sujetos que participan en dichos sistemas.

4. REQUISITOS DE LOS SISTEMAS DE ALTO RIESGO

El RIA establece los siguientes requisitos para que los sistemas de IA sean considerados de alto riesgo:

1. Establecimiento, implantación, documentación y mantenimiento de un sistema de gestión de riesgos en relación con los sistemas de IA de alto riesgo para la identificación y análisis de los riesgos conocidos y razonablemente previsibles, así como para la adopción de medidas adecuadas a tales riesgos. 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 seguri-

dad 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; y, 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).

2. Datos y gobernanza de datos. Nos referimos a la sujeción a prácticas de gobernanza y gestión de dato que incluyan prácticas adecuadas para la finalidad prevista en relación con el conjunto de datos de entrenamiento, validación y prueba. Ciertamente, 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 del artículo 10 del RIA siempre que se utilicen dichos conjuntos de datos. Ahora bien, 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) anterior; h) La detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.

Por otra parte, procede afirmar que, los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecen de errores y están 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 considerados en una combinación de estos.

A tal fin, 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. Ahora bien, 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 citado artículo 10, 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.

En todo caso, 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 del artículo 10 del RIA se aplicarán únicamente a los conjuntos de datos de prueba.

3. La elaboración de documentación técnica: 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. Asimismo, se redactará de modo que demuestre que el sistema de IA de alto riesgo cumple los requisitos

establecidos en la sección 1ª del Capítulo III 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. Deberá contener, 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 apartado 1 del artículo 11. Los organismos notificados aceptarán dicho formulario a efectos de la evaluación de la conformidad.

Por su parte, 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.

En todo caso, la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 del RIA 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 sección 2ª.

4. Conservación de registros: los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de acontecimientos (en adelante, "archivos de registro") a lo largo de todo el ciclo de vida del sistema.

Ahora bien, 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 im-

plicadas en la verificación de los resultados que se mencionan en el artículo 14, apartado 5.

5. Comunicación de información a los responsables del despliegue de forma transparente. 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.

A tal fin, 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. 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 del RIA.

6. Inclusión de supervisión humana. 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. A tal fin, el proveedor del sistema deberá definir las medidas adecuadas de supervisión humana antes de su introducción en el mercado o puesta en servicio. Dichas medidas deben garantizar que el sistema esté sujeto a limitaciones operativas incorporadas en el propio sistema, que éste no pueda desactivar; además, que responda al operador humano; y que las personas físicas a quienes se haya encomendado la supervisión humana tengan las competencias, la formación y la autoridad necesarias para desempeñar esa función. También resulta esencial garantizar que los sistemas de IA de alto riesgo incluyen 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 sobre: si deben intervenir, cuándo deben hacerlo y de qué manera, con el fin de evitar consecuencias negativas o riesgos, o de detener el sistema, si no funciona según lo previsto

Es, por ello, que 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.

Ahora bien, 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.

A efectos de la puesta en práctica de lo expuesto en líneas precedentes, 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 adecuada-

mente 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.

Ahora bien, para 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 artículo 14 del RIA 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.

Efectivamente, si atendemos a las importantes consecuencias que para las personas puede tener una correspondencia incorrecta efectuada por determinados sistemas de identificación biométrica; ello exige 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. En todo caso, este requisito no debe suponer una carga, ni retrasos innecesarios, pues, podría bastar con que las verificaciones que las distintas personas efectúen por separado se registren automáticamente en los registros generados por el sistema (considerando núm. 73 del RIA).

7. Desarrollo con niveles adecuados de precisión, solidez y ciberseguridad y que funcionen de manera uniforme de estas maneras a lo largo de todo el ciclo de su vida (por ejemplo, mediante el establecimiento de medidas técnicas y organizativas frente a errores, fallos, sesgos o violaciones de seguridad). 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.

En todo caso, para abordar los aspectos técnicos sobre la forma de medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 del artículo 15 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.

Asimismo, 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.

En este contexto, los sistemas de IA de alto riesgo deberán ser 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. Para ello, 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.

Ahora bien, 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. En todo caso, 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. Por su parte, 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.

5. OBLIGACIONES DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE SISTEMAS DE IA DE ALTO RIESGO Y DE OTROS SUJETOS

Atendiendo a 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 de este 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. Así, un operador puede actuar como distribuidor e importador al mismo tiempo.

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 y también sería el supuesto si dicha parte modifica sustancialmente un sistema de IA de alto riesgo que se haya introducido ya en el mercado o puesto en servicio; de tal forma que, el sistema modificado seguirá siendo un sistema de IA de alto riesgo de conformidad con este Reglamento. Ahora bien, si se modifica la finalidad prevista de un sistema de IA de uso general introducido ya en el mercado o puesto en servicio, pese a no ser un sistema de alto riesgo; sin embargo, el sistema modificado pasa a ser un sistema de IA de alto riesgo de conformidad con el Reglamento. Lo expuesto debe 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 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.

5.1. Obligaciones de los proveedores de sistema de IA de alto riesgo

Con respecto a los proveedores: Los proveedores de sistemas de IA de alto riesgo deben:

1. Velar por que sus sistemas de IA de alto riesgo cumplan los requisitos definidos en la sección 2ª del RIA;

2. Indicar 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;

3. Contar con un sistema de gestión de la calidad que cumpla lo dispuesto en el artículo 17;

4. Conservar la documentación a que se refiere el artículo 18; y de los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 19, cuando estén bajo su control. 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.

Si bien, cada Estado miembro determinará las condiciones en las que la documentación a que se refiere el apartado 1 del 18 del RIA 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.

Si bien, 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;

5. Asegurar 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.

6. Elaborar una declaración UE de conformidad en virtud de lo dispuesto en el artículo 47. Efectivamente, 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 este Reglamento en el sistema de gestión de la calidad establecido en dicho Derecho sectorial de la Unión. La complementariedad entre este Regla-

mento 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. Si bien, 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;

7. Colocar 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;

8. Cumplir las obligaciones de registro a que se refiere el artículo 49, apartado 1;

9. Adoptar las medidas correctoras necesarias y facilitarán la información exigida en el artículo 20;

10. Demostrar, previa solicitud motivada de la autoridad nacional competente, la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2ª;

11. Velar 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;

12. Establecer 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 2ª, 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, conser-

vación 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; 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; j) Los sistemas y procedimientos para llevar un registro de toda la documentación e información pertinente; k) La gestión de los recursos, incluidas medidas relacionadas con la seguridad del suministro; l) 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.

La aplicación de los aspectos mencionados en líneas precedentes 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 este Reglamento. Por su parte, 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.

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 artículo 17 del RIA 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.

13. Conservación de archivos de registro generados automáticamente. 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.

En su caso, 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.

14. Adopción de medidas correctoras y obligación de información. 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 este 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.

Si bien, 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.

En todo caso, para permitir la trazabilidad de los sistemas de IA de alto riesgo, verificar si cumplen los requisitos previstos en este 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.

15. Cooperación con las autoridades competentes. 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 ne-

cesarias para demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2ª, 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.

En todo caso, 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. Si bien, toda información obtenida por una autoridad competente con arreglo al artículo 21 del RIA se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78 del citado texto legal.

16. Nombramiento de representantes autorizados de los proveedores de sistemas de IA de alto riesgo. 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.

A tal fin, los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.

Por su parte, los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor y 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 de este Reglamento, el representante autorizado estará habilitado 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 2ª, 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 es-

tas emprendan en relación con el sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que estén presente; e) Cumplir, cuando proceda, 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.

En todo caso, 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 relación a todas las cuestiones relacionadas con la garantía del cumplimiento de este Reglamento.

Ahora bien, 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 RIA. 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.

De todas formas, aquellos proveedores que consideren que su sistema de IA no es alto riesgo antes de introducirlo en el mercado, deberán realizar y documentar una evaluación al respecto. Esta evaluación podrá ser requerida por las autoridades competentes.

Por otra parte, procede señalar que, cuando, con arreglo a las condiciones establecidas en este 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 de este 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 este Reglamento; en particular, en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo. 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 este Reglamento impone al proveedor y, en particular, debe garantizar que el sistema de IA integrado en el producto final cumpla los requisitos del mismo.

5.2. Obligaciones de los importadores

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 a tal fin deben:

1. Verificar que el proveedor del sistema de IA de alto riesgo ha llevado a cabo el procedimiento de evaluación de la conformidad pertinente a que se refiere el artículo 43.

2. Asegurarse que proveedor haya elaborado la documentación técnica de conformidad con el artículo 11 y el anexo IV.

3. Que 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.

4. 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 (comercializará) 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.

5. 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.

6. 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.

7. 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.

8. Los importadores proporcionarán a las autoridades competentes pertinentes, previa solicitud motivada, toda la información y la documentación, incluidas las referidas en el apartado 5 del artículo 23 del RIA, 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.

Y, 9. 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 estén presentes.

5.3. 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, han 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 2ª, 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 2ª.

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 2ª 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 del artículo 24 del RIA que sean necesarias para demostrar que dicho sistema cumple los requisitos establecidos en la sección 2ª.

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 estén presentes.

5.4. 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 del artículo 26 del RIA.

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 del artículo 26 del RIA 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. El responsable del despliegue, sin perjuicio de lo dispuesto en los apartados 1 y 2 del citado artículo 26, 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. Asimismo, 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 del artículo 72 del RIA, cuando se respeten las normas sobre sistemas, procesos y mecanismos de gobernanza interna de acuerdo con el Derecho pertinente en materia de servicios financieros.

Efectivamente, teniendo en 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, los responsables del despliegue deberán 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.

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. Ello 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. Ello, en todo caso, 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. En fin, 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 de este 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.

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

Esta obligación se cumplirá 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 al-

guno de los elementos enumerados en el apartado 1 del artículo 27 del RIA ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información.

Una vez, realizada la evaluación a que se refiere el citado apartado 1 del artículo 27, 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 citado 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 mencionado apartado 1 del artículo 27 complementará dicha evaluación de impacto relativa a la protección de datos.

En todo caso, 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.

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

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; y, d) Cuando se den las circunstancias definidas en el apartado 1 del artículo 27 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 de este Reglamento. En todo caso, este 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 apartado 1 del artículo 25 del RIA 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.

En el supuesto 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.

Por su parte, 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 apartado 4 del citado artículo 25 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.

En todo caso, 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.

Si bien, los apartados 2 y 3 del artículo 25 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.

Por otra parte, conviene precisar que, a lo largo de la cadena de valor de la IA, numerosas partes suministran a menudo no solo sistemas, herramientas y ser-

vicios 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.

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

5.6.1. Obligaciones de los proveedores 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. A tal fin, 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.

5.6.2. Obligaciones de los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica

1. 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.

Con el 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. 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.

En este contexto, 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.

2. 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.

La "ultrasuplantación" la define el artículo 3.60 del RIA como: "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".

3. 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.

4. La información a que se refieren los apartados 1 a 4 del artículo 50 de RIA 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.

5. Los citados apartados 1 a 4 del artículo 50 del RIA 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.

6. MODELOS DE IA DE USO GENERAL

Un modelo de IA de uso general es: 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 (artículo 3.63 del RIA).

Por su parte, 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 im-

pacto equivalente a los establecidos en la letra a), teniendo en cuenta los criterios establecidos en el anexo XIII.

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.

Una operación de coma flotante es: 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 (artículo 3.67 del RIA).

Ahora bien, 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.

En este contexto, 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 de este 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 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 poder llevar a cabo 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. Si bien, 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. Por su parte, 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 Anexo XIII de este Reglamento, como el número de parámetros modelo; la calidad o el tamaño del conjunto de datos de entrenamiento, por ejemplo, a través de criptofichas, los parámetros de referencia la evaluación de las capacidades del modelo, y 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.

En todo caso, 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.

En este contexto, también resulta necesario aclarar un procedimiento para la clasificación de un modelo de IA de uso general con riesgos sistémicos. De ahí que, deba 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. Para ello, 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 ámbito 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 resulta esencial para que la Oficina de IA pueda anticipar 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. Si bien, dicha información es especialmente importante cuando esté previsto divulgar un modelo de IA de uso general como modelo de este tipo de código, 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 este Reglamento.

Ahora bien, 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 deberá 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.

En este contexto, 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 este 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. Ciertamente, esta medida es, esencialmente, 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 propia Unión.

Asimismo, 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 previstas en este Reglamento o de otros Reglamentos. Por ello, 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.

Efectivamente, los proveedores de IA 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, en los terminos acordados. De forma que, deben establecerse medidas de transparencia proporcionadas, lo que incluye elaborar documentación y mantenerla actualizada, a la par que facilitar información sobre el modelo de IA de uso general para su uso por parte de los proveedores posteriores. En todo caso, 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 de este Reglamento. La Comisión debe estar facultada para modificar dichos anexos mediante actos delegados en función de los avances tecnológicos**.**

Ahora bien, 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. 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. Por su parte, 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.

De todas formas, la Comisión Europea puede modificar los umbrales para clasificar los modelos de IA de uso general -los modelos GPAI- como de riesgo sistémico (artículos 51.3 y 52.4 del RIA) [17].

6.1. Obligaciones de los proveedores de modelos de IA de uso general y de representantes autorizados de los proveedores de modelos de IA de uso general

6.1.1. Obligaciones de los proveedores de modelos de IA de uso general

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 RIA. 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 garan-

17 Para BARRIO ANDRÉS, M. (2024). "Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial", *op. cit.,* p. 3 "la Comisión tienen la oportunidad de utilizar pruebas del mundo real para establecer y definir el umbral de riesgo sistémico yendo más allá de los FLOP y añadiéndolos o sustituyéndolos por nuevos criterios de referencia".

tizar 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.

Por otra parte, con el fin de aumentar la transparencia en relación con los datos utilizados en el entrenamiento previo y en 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 puedan ejercer y hacer 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. Para tal fin, 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.

En lo referente a las obligaciones 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. Este Reglamento no afecta al cumplimiento de las normas en materia de derechos de autor previstas en el Derecho de la Unión.

Ahora bien, 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, in-

cluidas las nuevas fuentes de datos de entrenamiento, para cumplir las obligaciones relacionadas con la cadena de valor establecidas en este Reglamento.

Los proveedores de modelos de IA de uso general deberán:

1. Elaborar y mantener 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.
2. Elaborar y mantener 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.

   Las obligaciones dispuestas en el apartado 1, letras a) y b) del artículo 53 del RIA -esto es, las dos primeras- 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. Establecer 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.
4. Elaborar y poner 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.
5. 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.

6. 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 del RIA para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del artículo 53 del citado cuerpo legal, 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.
7. 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.

En todo caso, 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; y, 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.

6.1.2. Obligaciones de los representantes autorizados de los proveedores de modelos de IA de uso general

Antes de introducir en el mercado de la Unión un modelo de IA de uso general, los proveedores establecidos en terceros países tendrán que: 1. 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 de este 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.

Por otra parte, 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 de este Reglamento. Este 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.

En todo caso, la obligación establecida en el artículo 54 de la RIA (las obligaciones expuestas) 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.

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

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 RIA debe exigir a los proveedores que lleven a cabo las evaluaciones de los modelos necesarios, en particular antes de la primera introducción en el mercado, y que 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 mediante el establecimiento de políticas de gestión de riesgos, como procesos de rendición de cuentas y gobernanza, la puesta en práctica de la vigilan-

cia 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. Ciertamente, los proveedores de modelos de IA de uso general con riesgos sistémicos deben evaluar y mitigar los posibles riesgos sistémicos. Por lo que, si, a pesar de los esfuerzos por detectar y prevenir los riesgos relacionados con un modelo de IA de uso general pueda presentar riesgos sistémicos y 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. Por otra parte, 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. Así, la protección en esta materia relacionada con los riesgos sistémicos asociados al uso malintencionado o a los ataques debe tener, especialmente, 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 mediante medidas de seguridad operativa para la seguridad de la información, medidas específicas en el ámbito de la ciberseguridad, soluciones técnicas adecuadas y establecidas y controles de acceso cibernéticos y físicos, en función de las circunstancias pertinentes y los riesgos existentes.

Como hemos precisado en líneas precedentes, la Oficina de IA debe fomentar y facilitar la elaboración, revisión y adaptación de códigos de buenas prácticas, teniendo en cuenta los enfoques internacionales y debe colaborar con las autoridades nacionales competentes pertinentes y, cuando proceda, 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. En esencia, los códigos de buenas prácticas deben constituir una herramienta fundamental para el cumplimiento adecuado de las obligaciones previstas en eses Reglamento para los proveedores de modelos de IA de uso general. Resulta práctico que, los proveedores puedan operar sobre códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. La Comisión, mediante actos de ejecución, podrá 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. Sobre tales bases, 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. En todo caso, 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.

En este contexto, además de las obligaciones enumeradas en los artículos 53 y 54 del RIA, los proveedores de modelos de IA de uso general con riesgo sistémico deberán: a) Evaluar los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, lo que incluye la realización y documentación de pruebas de simulación de adversarios con el modelo con vistas a detectar y mitigar riesgos sistémicos; b) Evaluar y mitigar 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) Vigilar, documentar y comunicar, 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) Velar 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.

Como hemos tantas veces reiterado, 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 del RIA para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del artículo 55 del citado cuerpo legal hasta que se publique una norma armonizada. De nuevo procede indica que, 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.

En fin, toda información o documentación obtenida atendiendo a lo dispuesto en el artículo 55 del RIA, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78 del citado cuerpo legal.

7. LA NUEVA NORMATIVA EN MATERIA DE RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

7.1. La necesidad de regulación en materia de responsabilidad civil aplicable a los sistemas de IA

Antes de proceder al análisis de la citada materia de responsabilidad civil, hay que señalar, por una parte que, el derecho a presentar una reclamación ante una autoridad de vigilancia del mercado por toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el RIA, sin perjuicio de otras vías administrativas o judiciales de recurso. Atendiendo al 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 85 del RIA); y, por otra parte, de conformidad con las condiciones previstas en este 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.

De forma que, 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; y, el incumplimiento de cualquiera de las disposiciones 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; y, g) Las obligaciones de transparencia de los proveedores y responsables del despliegue con arreglo al artículo 50 (artículo 99 del RIA).

En cuanto a las multas administrativas, 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 de este Reglamento. Al tomar la decisión de 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; y, g) El presupuesto anual de la institución, órgano u organismo de la Unión (artículo 100) [18].

En todo caso, a 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 de 23 de octubre de 2019, relativo a la protección de las personas que informen sobre infracciones del Derecho de la Unión (artículo 87 del RIA). En España se ha aprobado en trasposición de la citada Directiva, la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

En este contexto, en el Libro Blanco sobre la IA de 19 de febrero de 2020, la Comisión se comprometió a promover la adopción de la IA y a abordar los riesgos

18 Por su parte, el artículo 101 del RIA hace referencia de forma específica a las multas a proveedores de modelos de IA de uso general, Así *"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; y, 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".*

asociados a algunos de sus usos fomentando la excelencia y la confianza. En el Informe sobre responsabilidad en materia de IA que acompaña al Libro Blanco, la Comisión señaló los retos específicos que plantea la IA con respecto a las normas vigentes en materia de responsabilidad civil. En sus Conclusiones sobre la configuración del futuro digital de Europa, de 9 de junio de 2020 el Consejo acogió con satisfacción la consulta sobre las propuestas políticas del citado Libro Blanco sobre la IA y pidió a la Comisión que presentase propuestas concretas. El 20 de octubre de 2020 el Parlamento Europeo adoptó una resolución legislativa de propia iniciativa en virtud del artículo 225 del Tratado de Funcionamiento de la Unión Europea (TFUE) en la que solicitaba a la Comisión que adoptase una propuesta relativa a un régimen de responsabilidad civil para la IA basado en el artículo 114 del TFUE.

Ciertamente, las normas nacionales en vigor en materia de responsabilidad civil, particularmente, las que se basan en la culpa, no resultan adecuadas para tramitar las denuncias de responsabilidad civil por daños causados por productos y servicios en los que se opera la IA. Con arreglo a dichas normas, las víctimas deben demostrar que ha habido una acción u omisión ilícita por parte de una persona y que ha causado el daño. Las características específicas de la IA, incluidas su complejidad, autonomía y opacidad (el denominado efecto de "caja negra"), pueden dificultar o hacer excesivamente costoso para las víctimas determinar cuál es la persona responsable y probar que se cumplen los requisitos para admitir una demanda de responsabilidad civil. En concreto, al reclamar una indemnización, las víctimas podrían tener que soportar unos costes iniciales muy elevados y enfrentarse a procedimientos judiciales más extensos en el tiempo, que los relativos a aquellos procesos que se inician sin relación alguna con la inteligencia artificial. Por lo tanto, las víctimas pueden verse disuadidas a intentar obtener una indemnización. Estas preocupaciones también han sido señaladas por el Parlamento Europeo en su Resolución de 3 de mayo de 2022 sobre la inteligencia artificial en la era digital.

Por otra parte, varios Estados miembros están analizando, o incluso planificando de manera concreta adoptar medidas legislativas sobre la responsabilidad civil en los supuestos en que medie IA. Lo que da lugar a una mayor fragmentación y a un aumento de los costes para las empresas que operan en la UE, especialmente a los de las pymes, impidiendo con ello la adopción de la IA en toda la Unión. Además, la ausencia de normas armonizadas a escala global de la UE para indemnizar los daños causados por los sistemas de IA, por una parte, los proveedores, operadores y demás sujetos que operan con sistemas de IA, tal como se regula en el RIA y, por otra, las personas perjudicadas se verían necesariamente abocados a trabajar con 27 regímenes de responsabilidad diferentes; lo que, daría lugar a distintos niveles de protección y falsearía la competencia entre las empresas de los distintos Estados miembros.

De ahí, que unas medidas armonizadas a escala de la UE mejorarían significativamente las condiciones para la introducción generalizada y el desarrollo de

tecnologías de IA en el mercado interior, evitarán la fragmentación y aumentarán la seguridad jurídica. Este valor añadido se generará, en particular, por la reducción de la fragmentación normativa y por proporcionar una mayor seguridad jurídica para las partes a la hora de entablar acciones de responsabilidad civil. Ciertamente, solo la actuación unificadora de la UE puede lograr de una manera adecuada y coherente el efecto deseado, como es, promover la confianza de los consumidores en los productos y servicios basados en la IA; evitando, asimismo, con ello las lagunas que puede existir en materia de responsabilidad civil vinculadas, precisamente, a las características específicas de la IA en todo el mercado interior.

Ello, a su vez, garantiza un nivel (mínimo) de protección uniforme para todas las víctimas (particulares y empresas), a la par de unos incentivos uniformes para prevenir daños y garantizar la rendición de cuentas.

Para tal fin, se ha aprobado la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificia (Directiva sobre responsabilidad en materia de IA) de 28 de septiembre de 2022.

Se ha optado por una Directiva, pues, ésta constituye el instrumento más adecuado para esta Propuesta, al proporcionar el efecto de armonización y la seguridad jurídica deseados, al tiempo que ofrece la flexibilidad necesaria para que los Estados miembros puedan integrar las medidas armonizadas sin fricciones con sus regímenes nacionales de responsabilidad civil.

En este contexto, teniendo en cuenta la política de la UE "legislar mejor", la Comisión ha sometido esta Propuesta de Directiva a una evaluación de impacto, que ha sido examinada por su Comité de Control Reglamentario. La reunión de este Comité de Control Reglamentario del 6 de abril de 2022 ha dado lugar a un dictamen favorable con varis observaciones. Se procedió a evaluar tres opciones políticas de actuación: Opción política 1: tres medidas para aliviar la carga de la prueba que recae sobre las víctimas que intentan presentar pruebas que apoyen su demanda de responsabilidad civil. Opción política 2: las medidas de la opción 1 + armonizar las normas de responsabilidad objetiva en los casos de uso de IA con un perfil de riesgo particular junto con un seguro obligatorio. Opción política 3: un enfoque por fases consistente en: una primera fase: en la que se adoptarían las medidas de la opción 1; y, una segunda fase: un mecanismo de revisión para reevaluar, en particular, la necesidad de armonizar la responsabilidad objetiva en los casos de uso de IA con un perfil de riesgo particular (posiblemente acompañado de un seguro obligatorio). Las opciones políticas se han comparado mediante un análisis multicriterio que tiene en cuenta su eficacia, eficiencia, coherencia y proporcionalidad. Los resultados del análisis multicriterio y de sensibilidad muestran que la opción política 3, que prevé el alivio de la carga de la prueba en las demandas relacionadas con la IA y la revisión específica en relación con la responsabilidad objetiva, posiblemente acompañada de un seguro obligatorio, ocupa un lugar preferente y es, por tanto, la opción política querida para

esta Propuesta. Esta opción política se entiende que garantiza que las víctimas de productos y servicios basados en la IA (personas físicas, empresas y cualquier otra entidad pública o privada) no estén menos protegidas que las víctimas de las tecnologías tradicionales. Lo cierto es que, con ello se aumentaría el nivel de confianza en la IA y, se fomentaría su adopción. Además, reduce la inseguridad jurídica y evita a la fragmentación normativa, ayudando así a las empresas -y sobre todo a las pymes- que quieran aprovechar todo el potencial del mercado único de la UE la posibilidad de una comercialización generalizada y transfronteriza de productos y servicios basados en la IA. En fin, esta opción política también crea condiciones mejores, para que las aseguradoras ofrezcan cobertura para actividades relacionadas con la IA; lo cual resulta crucial para que las empresas y, especialmente, las pymes gestionen sus riesgos.

Por otra parte, esta Propuesta de Directiva forma parte de un paquete de medidas para apoyar la adopción de la IA en Europa mediante el fomento de la excelencia y la confianza. Este paquete consta de tres líneas de trabajo complementarias: una propuesta legislativa por la que se establecen normas horizontales sobre los sistemas de inteligencia artificial (RIA); una revisión de las normas sectoriales y horizontales en materia de seguridad de los productos; y, normas de la UE para abordar las cuestiones de responsabilidad civil relacionadas con los sistemas de IA.

La seguridad y la responsabilidad civil son las dos caras de la misma moneda; y, aunque intervienen en momentos diferentes, se refuerzan mutuamente. No obstante, conviene precisar que, las normas para garantizar la seguridad y proteger los derechos fundamentales reducen los riesgos, pero no los eliminan por completo. En el supuesto que, se materialice tal riesgo, sigue existiendo la posibilidad que se produzcan daños. En tales casos, se aplicarán las normas sobre responsabilidad civil de esta Propuesta de Directiva.

Es, por ello, que el objetivo de esta Propuesta de Directiva sea la de promover la introducción generalizada de una IA fiable, a fin de aprovechar plenamente sus beneficios en el mercado interior. Esto se logra garantizando que las víctimas de daños causados por la IA obtengan una protección equivalente a la de las víctimas de daños causados por los demás productos. También reduce la inseguridad jurídica de las empresas que desarrollan o utilizan la IA en cuanto su posible exposición a responsabilidad civil, a la par que evita la aparición de adaptaciones a la IA a través de las normas nacionales en materia de responsabilidad civil que contribuyen a la fragmentación de la protección. Por otra parte, esta forma de operar, resulta ser un incentivo económico para cumplir con las normas de seguridad y, por ende, contribuyen a evitar que se produzcan daños. Además, esta Propuesta de Directiva contribuye al cumplimiento de los requisitos para sistemas de IA de alto riesgo impuestos por el RIA, ya que el incumplimiento de dichos requisitos constituye un elemento que, da lugar a un aligeramiento de la carga de la prueba y promueve una tecnología al servicio de las personas, uno de los tres pilares prin-

cipales de las orientaciones políticas y los objetivos anunciados en la Comunicación titulada "Configurar el futuro digital de Europa".

Ahora bien, la Comisión adopta un enfoque holístico en su política de responsabilidad en materia de IA; de ahí que, proponga adaptaciones de esta Propuesta de Directiva con la responsabilidad del productor por productos defectuosos (de ahí, la aprobación de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por producto defectuosos de la misma fecha de 28 de septiembre de 2022). Y, también resulta coherente esta Propuesta de Directiva con las normas generales y sectoriales propuestas en materia de seguridad de los productos aplicables a las máquinas y a sus partes y accesorios y a los equipos radioeléctricos que emplean IA.

En este contexto, procede señalar que ambas iniciativas políticas (responsabilidad civil y responsabilidad por productos defectuosos) están estrechamente vinculadas y forman de un paquete; si bien, las demandas que entran en sus ámbitos de aplicación, se refieren a diferentes tipos de responsabilidad.

Así, la Directiva sobre responsabilidad por los daños causados por productos defectuosos cubre la responsabilidad objetiva del productor por productos defectuosos, lo que da lugar a una indemnización por determinados tipos de daños, principalmente sufridos por particulares. Mientras que la Propuesta de Directiva de responsabilidad civil cubre las demandas nacionales de responsabilidad fundamentadas, principalmente, en la culpa de cualquier persona con el fin de indemnizar por cualquier tipo de daño y a cualquier tipo de víctima. Se complementan entre sí para formar un sistema general de responsabilidad civil eficaz. Juntas contribuyen a generar confianza en la IA (y otras tecnologías digitales), garantizando que las víctimas reciban una indemnización efectiva si, a pesar de los requisitos preventivos del RIA y otras normas de seguridad, se producen daños.

Ahora bien, partiendo de la pretensión de generar confianza en la IA y promover su adopción, esta Propuesta de Directiva resulta también complementaria con la Ley de ciberresiliencia que, asimismo, tiene por objeto fortalecer la confianza en los productos con elementos digitales, reduciendo las vulnerabilidades cibernéticas y proteger mejor a las empresas y a los usuarios consumidores. Por supuesto, no afecta a las normas establecidas por la Ley de Servicios Digitales, que establecen un marco integral y plenamente armonizado para las obligaciones de diligencia debida para la toma de decisiones algorítmica por parte de las plataformas en línea, incluida su exención de responsabilidad para los prestadores de servicios intermediarios.

Por otra parte, al promover esta Propuesta de Directiva con su contenido la adopción de la IA se vincula a las iniciativas de la Estrategia de Datos de la UE. También refuerza el papel de la Unión para ayudar a configurar las normas y estándares mundiales y, promover una IA fiable que sea coherente con los valores e intereses de la Unión. Esta Propuesta de Directiva, igualmente, tiene vínculos indirectos con el "Pacto Verde Europeo".

En particular, las tecnologías digitales, incluida la IA, son un factor fundamental para alcanzar los objetivos de sostenibilidad del Pacto Verde en muchos sectores diferentes (como la asistencia sanitaria, el transporte, el medio ambiente y la agricultura).

En esta línea, procede, asimismo, indicar que, esta Propuesta de Directiva repercutirá positivamente en los Objetivos de Desarrollo Sostenible (ODS), ya que una legislación eficaz en materia de transparencia, rendición de cuentas y derechos fundamentales orientará el potencial de la IA en beneficio de las personas y de la sociedad hacia la consecución de los ODS y de las metas correspondientes.

Sobre tales bases, partiendo de la base que, una de las funciones más importantes de las normas de responsabilidad civil es garantizar que las víctimas de daños puedan reclamar una indemnización; estas normas contribuyen a garantizar una indemnización efectiva, la protección del derecho a la tutela judicial efectiva, y la existencia de un juez imparcial (artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea); al tiempo que incentivan a las personas que, potencialmente, puedan incurrir en responsabilidad civil a prevenir los daños y perjuicios con el fin de evitar que se genere la responsabilidad.

En particular, esta Propuesta contribuye a proteger los derechos fundamentales como: el derecho a la vida (artículo 2 de la Carta); el derecho a la integridad física y mental (artículo 3); y, el derecho a la propiedad (artículo 17). Además, en función del sistema y las tradiciones de Derecho civil de cada Estado miembro, las víctimas podrán reclamar una indemnización por los daños causados a otros intereses jurídicos, como las violaciones de la dignidad personal (artículos 1 y 4 de la Carta); el respeto de la vida privada y familiar (artículo 7); el derecho a la igualdad (artículo 20); y, la no discriminación (artículo 21).

Ahora bien, procede señalar que, esta Propuesta complementa otras vertientes de la política de IA de la Comisión basadas en requisitos preventivos normativos y de supervisión destinados directamente a evitar violaciones de los derechos fundamentales (como la discriminación): el RIA, el Reglamento General de Protección de Datos, la Ley de Servicios Digitales y la legislación de la UE sobre no discriminación e igualdad de trato.

Por otra parte, resulta importante indicar que, al mismo tiempo, con esta Propuesta no se pretende crear, ni armonizar los deberes de diligencia, ni la responsabilidad civil de las distintas entidades cuya actividad está regulada por dichos actos jurídicos; y, por lo tanto, no crea nuevos tipos de demandas de responsabilidad, ni afecta a las exenciones de responsabilidad previstas en esos otros actos jurídicos. Esta Propuesta solo introduce "aligeramientos" de la carga de la prueba para las víctimas de daños causados por sistemas de IA en las demandas, que pueden fundamentarse en la legislación nacional o en estas otras leyes de la UE. Al complementarse con estas otras vertientes, esta Propuesta protege el dere-

cho de la víctima a una indemnización en virtud del Derecho privado, incluidas las indemnizaciones por violaciones de los derechos fundamentales.

Esta Propuesta de Directiva sigue un enfoque de armonización mínima, permitiendo a los demandantes en casos de daños causados por sistemas de IA invocar normas más favorables del Derecho nacional. Así pues, las legislaciones nacionales podrán, por ejemplo, mantener la inversión de la carga de la prueba en el contexto de regímenes nacionales de responsabilidad subjetiva (basada en la culpa), u optar por regímenes nacionales de responsabilidad sin culpa (conocida como "responsabilidad objetiva") -de los que ya existe una gran variedad en las legislaciones nacionales-, que puedan resultar de aplicación a los daños causados por sistemas de IA.

Ahora bien, tal enfoque contrasta con la Propuesta de Directiva de daños por productos defectuosos que, es de la armonización máxima y, opera siempre sobre un sistema de responsabilidad objetiva, frente a la Propuesta de Directiva de responsabilidad en materia de IA que parte, en principio, de una responsabilidad basada en la culpa.

En todo caso, debe garantizarse la coherencia con el RIA recientemente publicado en el DOUE. Procede, por tanto, que cuando se apruebe esta Propuesta de Directiva, se utilice las mismas definiciones con respecto a los sistemas de IA, los proveedores, distribuidores, importadores. Además, hay que recordar que, esta Propuesta de Directiva solo debe abarcar las demandas por daños y perjuicios que hayan sido causados por una información de salida -o por la no producción de una información de salida- imputable a un sistema de IA cuando medie culpa de una persona, por ejemplo, el proveedor o el importador, distribuidos con arreglo al RIA.

7.2. Objeto y ámbito de aplicación de la Propuesta de Directiva

El objeto de esta Propuesta de Directiva es mejorar el funcionamiento del mercado interior mediante el establecimiento de requisitos uniformes para determinados aspectos de la responsabilidad civil extracontractual por los daños causados con mediación de sistemas de IA. Da continuidad a la Resolución del Parlamento Europeo 2020/2014 y adapta el Derecho privado a las necesidades de la transición a la economía digital. La elección de instrumentos jurídicos adecuados es limitada, dada la naturaleza de la cuestión de la carga de la prueba y las características específicas de la IA, que plantean un problema con respecto a las normas de responsabilidad existentes. A este respecto, esta Propuesta de Directiva aligera o alivia la carga de la prueba de manera muy específica y proporcionada mediante el uso de la exhibición y las presunciones refutables (*iuris tantum*).

Asimismo, establece, para aquellos que soliciten una indemnización por daños y perjuicios la posibilidad de obtener información sobre los sistemas de IA de alto riesgo, que debe registrarse o documentarse de conformidad con el RIA. Ade-

más, las presunciones refutables ofrecen a quienes soliciten una indemnización por los daños causados por sistemas de IA una carga de la prueba más razonable y, una oportunidad de que sus demandas de responsabilidad civil prosperen.

Ahora bien, estas herramientas jurídicas no son *per se* novedosas, pues, pueden encontrarse en los sistemas legislativos nacionales. Por lo tanto, estas herramientas nacionales constituyen puntos de referencia útiles sobre cómo abordar las cuestiones planteadas por la IA en relación con las normas de responsabilidad civil en vigor; de forma que, se interfiera lo menos posible en los diferentes regímenes jurídicos nacionales. Además, frente a instrumentos jurídicos como la inversión de la carga de la prueba o una presunción irrefutable (*iuris et de iure*), se ha preferido optar por medidas específicas para aligerar la carga de la prueba en forma de presunciones refutables, por tratarse de medios pragmáticos y adecuados para ayudar a las víctimas a soportar la carga de la prueba de una forma más específica y proporcionada.

A tal fin, el artículo 1 de la Propuesta de Directiva se refiere al objeto y su ámbito de aplicación. Así, se aplica a las demandas civiles de responsabilidad extracontractual por daños y perjuicios causados por un sistema de IA, cuando dichas demandas se interpongan en el marco de regímenes de responsabilidad subjetiva o por culpa. Esto es a los regímenes que establecen la responsabilidad legal de indemnizar los daños causados de forma deliberada (dolo) o por un acto u omisión negligente (culpa).

Por lo que, las medidas previstas en esta Propuesta Directiva pueden encajar sin problemas en los sistemas de responsabilidad civil nacionales en vigor, ya que reflejan un enfoque que no se centra en la definición de conceptos fundamentales como "culpa" o "daño", dado que el significado y alcance de estos conceptos varía considerablemente entre los Estados miembros de la UE.

De forma que, que se puede señalar que, esta Propuesta de Directiva no afecta a las normas nacionales o de la Unión que determinan, por ejemplo, qué parte ha de soportar la carga de la prueba; qué grado de certeza es necesario para que haya fuerza probatoria; o cómo se define la culpa. Tampoco afecta a las normas vigentes que regulan las condiciones de responsabilidad en el sector del transporte, ni a las establecidas por la Ley de Servicios Digitales. Aunque esta Propuesta de Directiva no se aplica a la responsabilidad penal, puede resultar aplicable a la responsabilidad civil del Estado. Ciertamente, las autoridades estatales también están afectadas por las disposiciones del RIA como sujetos de las obligaciones, que en ella se establecen. Ahora bien, esta Propuesta de Directiva no se aplica retroactivamente, sino únicamente a las demandas de indemnización por daños y perjuicios que tengan lugar a partir de la fecha de su transposición.

Por su parte, el artículo 2, apartado 6, letra b) establece que las demandas por daños y perjuicios, pueden ser interpuestas no sólo por el perjudicado, sino también por las personas que lo hayan sucedido o se hayan subrogado en sus derechos. La subrogación es la asunción por un tercero (como una compañía de

seguros) del derecho legal de otra parte a cobrar una deuda o una indemnización por daños y perjuicios. De este modo, una persona tiene derecho a hacer valer los derechos de otra en beneficio propio. La subrogación también abarca a los herederos de una víctima fallecida. Además, el artículo 2, apartado 6, letra c) dispone que también puede interponer una demanda por daños y perjuicios una persona que actúe en nombre de una o varias partes perjudicadas de conformidad con el Derecho de la Unión o nacional. Esta disposición tiene por objeto brindar más posibilidades a las personas perjudicadas por un sistema de IA, que un tribunal conozca de su demanda tanto en aquellos casos de interposición de una demanda individual, o de una demanda conjunta con los beneficios de escala que puede conllevar.

En este contexto, para que las víctimas de daños causados por sistemas de IA puedan hacer valer sus derechos en relación con esta Propuesta de Directiva mediante acciones de representación en su artículo 6 se modifica el anexo I de la Directiva (UE) 2020/1828.

Ahora bien, esta Propuesta de Directiva se refiere al demandante y también a demandante potencial. El primero lo define el artículo 3.6 como: "persona que interpone una demanda por daños y perjuicios y que: a) se ha visto perjudicada por la información de salida de un sistema de IA o por la no producción por parte de dicho sistema de una información de salida que debería haber producido; b) ha sucedido a una persona perjudicada o se ha subrogado en su derecho en virtud de una ley o contrato; o c) actúa en nombre de uno o varios perjudicados, de conformidad con el Derecho de la Unión o nacional"; y el segundo el "demandante potencial" en el número 7 del citado precepto como: "persona física o jurídica que está considerando la posibilidad de presentar una demanda por daños y perjuicios, pero que aún no lo ha hecho". En fin, también ofrece un concepto de "demandado": "la persona contra la que se interpone una demanda por daños y perjuicios" (artículo 3.8). Este último es el sujeto responsable y se refiere: al proveedor que remite para su definición a la contenida en el artículo 3.3 del RIA -expuesta otro apartado de este estudio-; y, a las personas con las mismas obligaciones impuestas al proveedor a las que se refiere el artículo 4.2 de la Propuesta de Directiva con remisión, asimismo, al artículo 3 números 4 -responsable del despliegue-; número 5 -representante autorizado; número 6 -importador-; número 7 -distribuidos-; y, número 8 -operador-, todos ellos, igualmente, definidos en líneas precedentes. Aunque la Propuesta de Directiva sigue hablando de usuarios, estos sujetos ya no se mencionan en el RIA, aunque sí en la Propuesta de Reglamento. Por lo que, no procede aludir a ellos.

Ahora bien, esta Propuesta de Directiva parte de la aplicación de los regímenes de responsabilidad subjetiva o por culpa previstos en los ordenamientos nacionales de cada Estado miembro; a lo que añade como novedad dos aspectos fundamentales la exhibición de pruebas (artículo 3) y el régimen de presunciones (artículo 4) con el objeto de aliviar *versus* aligerar la carga de la prueba del

demandante o potencial demandante (víctima) que tienen que aportar en los procesos de responsabilidad civil, cuando los sistemas de IA son, principalmente, de alto riesgo; todo ello sin perjuicio de la existencia de otros recursos jurídicos en el ámbito interno (nacional) que favorecen también la posición jurídica del demandante (víctima).

En fin, la regulación de esta Propuesta de Directiva van destinada, principalmente, a los sistemas de IA de alto riesgo; sin embargo, en la Propuesta de Directiva sobre responsabilidad por productos defectuosos los daños podrán ser causados por cualquier sistema inteligente con independencia del riesgo y, quedan sometidos todos ellos, igualmente, a las reglas de exhibición de pruebas (artículo 8) y a un régimen de presunciones de defecto y/o relación de causalidad entre éste y el daño (artículo 9) [19].

Recordemos que, al ser de armonización mínima, la citada Propuesta de Directiva de Responsabilidad Civil no define daño, ni culpa, pues, remite a la regulación nacional de cada Estado miembro [20].

7.3. Reglas procesales previstas en la Propuesta de Directiva

7.3.1. "Exhibición de pruebas" o "deber de aportar la información probatoria"

Esta Propuesta de Directiva pretende proporcionar a las personas que soliciten una indemnización por los daños causados por sistemas de IA de alto riesgo medios eficaces para determinar las personas potencialmente responsables y las pruebas pertinentes de cara a una demanda. Al mismo tiempo, estos medios sirven para excluir a posibles demandados determinados erróneamente, ahorrando tiempo y costes a las partes implicadas y reduciendo la carga de trabajo de los tribunales. A este respecto, en los supuesto de sistemas de alto riesgo como indica MARTÍN CASALS "se posibilita a las victimas un derecho de acceso a la información que estén en poder de las empresas y proveedores y que resultan necesarias para su reclamación ("exhibiciones de pruebas")" [21]. Así, el artículo 3, apartado 1 de la Propuesta de Directiva establece que un órgano jurisdiccional puede orde-

19 Vid., un análisis de ambas Propuestas en ATIENZA NAVARRO, Mª.L. (2024). "¿Daños nuevos, reglas nuevas para su indemnización? Responsabilidad civil e inteligencia artificial a la luz de las demás propuestas de la Unión Europea", R*evista Aranzadi de Derecho y Nuevas Tecnologías, número 64, enero-abril*, pp. 57 a 76.

20 Para ORTIZ FERNÁNDEZ, M. (2024). "La adaptación del derecho de daños a la inteligencia artificial: la Propuesta de Directiva sobre responsabilidad", *Revista de internet, derecho y política, núm. 40, marzo*, p.7 resulta necesario "que se incluyese en la propuesta una definición de daños indemnizables por dos motivos: por un lado, precisamente, por la gran diversidad existente en los Estado miembros que bien podría vaciar de contenido, en algún supuesto, la posible indemnización al no contemplar determinados conceptos. Y, por otro lado, por las peculiaridades existentes en el sector que nos ocupa, tanto por la cuantía de los perjuicios como por la amplia tecnología de daños".

21 MARTÍN CASALS, M. (2023). "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *op. cit.*, p. 71.

nar la exhibición de pruebas pertinentes relativas a sistemas de IA de alto riesgo específicos de los que se sospeche que han causado daños, ya sea a petición de un demandante potencial que haya solicitado previamente a un proveedor, a una persona sujeta a las obligaciones de un proveedor que exhiba las pruebas pertinentes que obran en su poder sobre un determinado sistema de IA de alto riesgo del que se sospeche que ha causado daños, pero cuya solicitud haya sido denegada, o a petición de un demandante. En apoyo de esta solicitud, el demandante potencial deberá presentar hechos y pruebas suficientes para sustentar la viabilidad de una demanda de indemnización por daños y perjuicios.

De forma que, las solicitudes de pruebas se dirigen al proveedor de un sistema de IA, a una persona sujeta a las obligaciones del proveedor; representantes autorizados de los proveedores de sistemas de IA de alto riesgo; importadores; y, distribuidores (artículos 21 a 25 del RIA).

Por tanto, las solicitudes deben estar respaldadas por hechos y pruebas suficientes para acreditar la viabilidad de la demanda por daños y perjuicios prevista y las pruebas solicitadas deben estar a disposición de los destinatarios, y, no pueden dirigirse a partes que no estén sujetas a obligaciones en virtud del RIA y que, por tanto, no tengan acceso a las pruebas.

De conformidad con el artículo 3, apartado 2 el demandante solo puede solicitar la exhibición de pruebas a proveedores o usuarios (que ya no se contienen referencia a ellos en el RIA), que no sean demandados en caso de que se hayan realizado sin éxito todos los intentos proporcionados de obtener las pruebas del demandado. Para que los medios judiciales sean eficaces, el artículo 3 apartado 3 de la Propuesta de Directiva establece que un órgano jurisdiccional también puede ordenar la conservación de tales pruebas. Por su parte, el mencionado artículo 3, apartado 4 párrafo primero establece al respecto que, el órgano jurisdiccional únicamente puede ordenar dicha exhibición en la medida necesaria para sustentar la demanda, dado que la información podría constituir una prueba fundamental para la demanda de la persona perjudicada en caso de daños en los que hayan mediado sistemas de IA.

Ahora bien, como se limita la obligación de exhibición o conservación a las pruebas necesarias y proporcionadas: el mencionado artículo 3, apartado 4 párrafo primero pretende, precisamente, garantizar la proporcionalidad en la exhibición de las pruebas, esto es, limitar la exhibición al mínimo necesario e impedir solicitudes genéricas. En fin, este artículo 3, apartado 4, párrafos segundo y tercero tiene también por objeto lograr un equilibrio entre los derechos del demandante y la necesidad de garantizar que dicha exhibición esté sujeta a garantías que protejan los intereses legítimos de todas las partes interesadas, como los secretos comerciales o la información confidencial. En el mismo contexto, el citado artículo 3, apartado 4, párrafo cuarto tiene por objeto garantizar que la persona sujeta a la orden de exhibición o conservación tenga remedios procesales a su disposición. Y, el apartado 5, del tantas veces mencionado, artículo 3 introduce

una presunción de incumplimiento de un deber de diligencia[22]. El demandado incumple la orden del tribunal nacional relativa a la exhibición o conservación de la información necesaria para la prueba y, en consecuencia, la norma presume que se ha incumplido un deber de diligencia (de conducta diligente); lo que da lugar a que se consideren probados los hechos sobre los que se requiere información probatoria. De ahí que, estemos ante una herramienta procesal aplicable únicamente a aquellos supuestos en que el propio demandado en una demanda por daños y perjuicios sea quien soporte las consecuencias del incumplimiento de una solicitud de exhibición o conservación de pruebas. Al demandado le asistirá el derecho de refutar, desvirtuar esa presunción mediante prueba en contrario. En todo caso, la medida establecida en este apartado tiene por objeto promover la exhibición y, asimismo, acelerar los procedimientos judiciales.

Sobre tales bases, procede señalar que, el acceso a información sobre sistemas de IA de alto riesgo específicos de los que se sospecha que han causado daños y perjuicios, es un factor importante a la hora de determinar si procede reclamar una indemnización y de fundamentar las demandas de indemnización. Además, en el caso de los sistemas de IA de alto riesgo, el RIA establece requisitos específicos de documentación, información y registro, pero no otorga al perjudicado el derecho a acceder a dicha información. De ahí, la importancia de establecer normas sobre la exhibición de los medios de prueba pertinentes por parte de quienes los tengan a su disposición a efectos de determinar la responsabilidad. Esto también debe ofrecer un incentivo adicional para cumplir los requisitos pertinentes establecidos en el RIA para documentar o registrar la información pertinente.

En este contexto, no cabe duda que son muchas las personas que suele participar en el diseño, el desarrollo, la introducción generalizada y el funcionamiento de sistemas de IA de alto riesgo: lo que, hace difícil que los perjudicados puedan identificar a la persona potencialmente responsable de los daños causados y, demuestren que se cumplen las condiciones para interponer una demanda por daños y perjuicios.

Para que los perjudicados puedan determinar si una demanda por daños y perjuicios es fundada, conviene conceder a los demandantes potenciales el derecho a solicitar a un órgano jurisdiccional que ordene la exhibición de las pruebas pertinentes antes de presentar una demanda por daños y perjuicios en los términos expuestos.

Dicha exhibición solo debe ordenarse cuando el demandante potencial presente hechos e información suficientes para acreditar la viabilidad de una demanda por daños y perjuicios y haya presentado previamente una solicitud al provee-

22 El artículo 3.9 de la Propuesta de Directiva define el deber de diligencia como: *"una norma de conducta exigida establecida por el Derecho nacional o de la Unión con el fin de evitar daños a bienes jurídicos reconocidos a nivel nacional o de la Unión, incluidos la vida, la integridad física, la propiedad y la protección de los derechos fundamentales".*

dor, a la persona sujeta a las obligaciones de un proveedor para que exhiba dichas pruebas que obran en su poder sobre sistemas de IA de alto riesgo específicos de los que se sospeche que han causado daños y perjuicios, y que esta solicitud haya sido denegada.

Desde un punto de vista procesal y económico, esta orden de exhibición debe llevar a una reducción de los litigios innecesarios y evitar costes a los posibles litigantes causados por demandas sin fundamento o con pocas posibilidades de prosperar. La negativa del proveedor, de la persona sujeta a las obligaciones de un proveedor o de un distribuidor, importador, responsable previa a la solicitud de exhibición de pruebas al órgano jurisdiccional no debe dar lugar a la presunción de incumplimiento de las obligaciones de diligencia pertinentes por parte de la persona que deniegue dicha exhibición.

Ahora bien, desde un punto de vista objetivo, la limitación de la exhibición de pruebas en lo que respecta a los sistemas de IA de alto riesgo es coherente con el RIA, que establece determinadas obligaciones específicas en materia de documentación, conservación de registros e información para los operadores que participan en el diseño, el desarrollo y la introducción de sistemas de IA de alto riesgo. Esta coherencia también garantiza la proporcionalidad necesaria al evitar que los operadores de sistemas de IA que planteen un riesgo menor o nulo tengan que documentar la información con un grado de detalle similar al exigido en el caso de los sistemas de IA de alto riesgo en virtud del RIA.

Sobre tales bases, los órganos jurisdiccionales nacionales deben poder ordenar, en el transcurso de un proceso civil, la exhibición o conservación de pruebas pertinentes relacionadas con los daños causados por sistemas de IA de alto riesgo a personas que ya estén obligadas a documentar o registrar información en virtud del RIA, ya se trate de proveedores, de personas sujetas a las mismas obligaciones que los proveedores o de distribuidores, importadores, representantes de un sistema de IA, ya sean estos demandados o terceros con respecto a la demanda.

En todo caso, puede darse situaciones en las que las pruebas pertinentes para el asunto obren en poder de entidades que no sean parte en la demanda por daños y perjuicios, pero que estén obligadas a documentar o registrar dichas pruebas de conformidad con el RIA. Por lo tanto, resulta necesario fijar las condiciones en que se puede ordenar a tales terceros con respecto a la demanda que exhiban las pruebas pertinentes.

Ahora bien, para mantener el equilibrio entre los intereses de las partes en la demanda por daños y perjuicios y los de los terceros afectados, los órganos jurisdiccionales deben ordenar la exhibición de pruebas únicamente cuando sea necesario y proporcionado para sustentar la demanda real o potencial por daños y perjuicios. A este respecto, la exhibición solo debe referirse a las pruebas que sean necesarias para adoptar una decisión sobre la correspondiente demanda por daños y perjuicios.

Por otra parte, para garantizar la proporcionalidad de tales medidas de exhibición o conservación, los órganos jurisdiccionales nacionales deben disponer de medios eficaces para salvaguardar los intereses legítimos de todas las partes implicadas; así, la protección de los secretos comerciales en el sentido de la citada Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8 de junio y de la información confidencial como la relacionada con la seguridad pública o nacional. Por lo que respecta a los secretos comerciales o a los presuntos secretos comerciales que el órgano jurisdiccional haya considerado como confidenciales en el sentido de la Directiva (UE) 2016/943, los órganos jurisdiccionales nacionales deben estar facultados para adoptar medidas específicas que garanticen la confidencialidad de los secretos comerciales durante y después del proceso, al tiempo que se logra un equilibrio justo y proporcionado entre el interés del poseedor del secreto comercial en mantener el secreto y el interés de la persona perjudicada. Esto debe incluir medidas para restringir el acceso a los documentos que contengan secretos comerciales y el acceso a las audiencias o los documentos y sus transcripciones a un número limitado de personas. Al decidir sobre tales medidas, los órganos jurisdiccionales nacionales deben tener en cuenta la necesidad de garantizar el derecho a la tutela judicial efectiva y a un juez imparcial, los intereses legítimos de las partes y, en su caso, de terceros, así como el perjuicio que pudiera ocasionarse a cualquiera de las partes o, en su caso, a terceros, como consecuencia de que se acuerden o no dichas medidas. En todo caso, a fin de garantizar una aplicación proporcionada de las medidas de exhibición dirigidas a terceros en las demandas por daños y perjuicios, los órganos jurisdiccionales nacionales deben ordenar la exhibición por parte de terceros únicamente si las pruebas no pueden obtenerse del demandado.

Aunque, los órganos jurisdiccionales nacionales disponen de medios para hacer ejecutar sus órdenes de exhibición a través de diversas medidas, tales medidas de ejecución podrían retrasar las demandas por daños y perjuicios y, por tanto, generar gastos adicionales para los litigantes. Para los perjudicados, tales retrasos y gastos adicionales pueden dificultar su acceso a la tutela judicial efectiva. Por lo tanto, cuando un demandado en una demanda de indemnización por daños y perjuicios no exhibe las pruebas a su disposición según lo ordenado por un órgano jurisdiccional, procede establecer, la mencionada presunción de incumplimiento de las obligaciones de diligencia que dichas pruebas debían demostrar. Esta presunción refutable reducirá la duración de los litigios y redundará en una mayor eficiencia de los procedimientos judiciales. Ahora bien, el demandado debe poder refutar esta presunción presentando pruebas en contrario.

Ciertamente, con el objeto de hacer frente a las dificultades para demostrar que un dato de entrada concreto del que es responsable la persona potencialmente responsable dio lugar a una información de salida específica de un sistema de IA que, a su vez, provocó el daño en cuestión, procede establecer, en determinadas condiciones, una presunción de causalidad.

En este contexto, la operatividad de la exhibición de pruebas y de la presunción en las demandas basadas en la culpa parte de la premisa que, el demandante normalmente tiene que probar el daño, la acción u omisión humana que determina la culpa del demandado y el vínculo de causalidad entre ambos, pues, esta Propuesta de Directiva no armoniza las condiciones en las que los órganos jurisdiccionales nacionales establecen la culpa; y, en consecuencia, sigue rigiéndose por el Derecho nacional aplicable

7.3.2. Presunción de relación de causalidad en caso de culpa (responsabilidad subjetiva)

En lo que respecta a los daños causados por sistemas de IA, esta Propuesta de Directiva pretende proporcionar un fundamento eficaz para reclamar una indemnización en relación con la culpa consistente en el incumplimiento de un deber de diligencia en virtud del Derecho de la Unión o nacional; y, por ende, facilitar la interposición de demandas por los daños producidos por un sistema de IA, a la par que reduce los costes procesales para los demandantes (víctimas).

No debemos olvidar que, puede resultar difícil para los demandantes probar que existe un nexo causal entre dicho incumplimiento y la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA que haya dado lugar a los daños en cuestión. Por lo tanto, en el artículo 4, apartado 1, se ha establecido una presunción refutable de causalidad específica en relación con este nexo causal. Esta presunción, aunque es menos gravosa para el demandado; viene, no obstante, a dar respuesta a la necesidad de una indemnización justa para la víctima.

Ahora bien, el demandante debe demostrar la culpa del demandado con arreglo a las normas nacionales o de la Unión aplicables. Esta culpa puede determinarse, por ejemplo, por incumplimiento de un deber de diligencia dispuesto en el RIA; o de otras normas establecidas a escala de la Unión, como las que regulan el uso de la supervisión y la toma de decisiones automatizadas para el trabajo en plataformas, o las que regulan el funcionamiento de aeronaves no tripuladas.

En este contexto, el artículo 4.1 de la Propuesta de Directiva establece como requisitos para que opere la presunción *iuris tantum* de causalidad entre la culpa del demandado y la producción o no producción de resultados en un sistema de IA los siguientes: 1. La culpa del demandado o de una persona cuyo comportamiento sea responsable el demandado. Consiste en el incumplimiento del mencionado deber de diligencia -que la información sea solicitada por el demandante y que se niegue a exhibirla el demandado-. En todo caso, ha de quedar probada, sea por parte del demandante, sea mediante el mecanismo de presunción de culpa que establece el artículo 3 de esta Propuesta. Efectivamente, el órgano jurisdiccional puede presumir la culpa sobre la base del incumplimiento de una orden judicial de exhibición o conservación de pruebas con arreglo al citado artículo 3

apartado 5. No obstante, solo procede introducir una presunción de causalidad, cuando pueda considerarse probable que la culpa en cuestión haya influido en la información de salida del sistema de IA pertinente -o en la ausencia de la información de salida-; lo cual puede evaluarse en función de las circunstancias generales del caso[23]. 2. Al mismo tiempo, resulta necesario que pueda considerarse razonablemente probable, basándose en las circunstancias de caso, que la culpa ha influido en los resultados producidos por el sistema de IA o en la producción de resultado por parte del sistema de IA[24]. De forma que, basta la razonable probabilidad de producción o no de información en el sistema de IA para acreditar la culpa y la relación de causalidad con tal resultado; Y, 3. El demandante aún tiene que demostrar que el sistema de IA (es decir, la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA) ha causado los daños.

Atendiendo a lo expuesto, coexisten dos nexos causales, o como también dice la doctrina, el nexo causal se divide en dos partes: el primer nexo causal tendría lugar entre la producción o no producción de resultados por parte de la IA y los daños generados al demandante (víctima). Por lo que, corresponde demostrar esta parte del nexo causal a la propia víctima (artículo 4.1. letra c); y, el segundo nexo causal o segunda parte del nexo causal entre la culpa del demandado y la producción o no producción de resultados por parte del sistema de IA. Para ello, se presume iuris tantum el nexo causal entre la culpa y el resultado o ausencia de resultados producidos por la IA, si operan los dos primeros requisitos expuestos en líneas precedentes (la culpa del demandado y se considere razonablemente probable que la culpa ha influido o no en los resultados producidos por la IA -artículo 4.1 letras a) y b))[25].

---

23 NAVAS NAVARRO, S. (2022). "Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial", *Revista CESCO de Derecho de Consumo, núm. 44*, p. 36 precisa que lo que debe probar el demandante es el criterio de imputación; y añade que "no es descartable que también haya influido en la Propuesta de Directiva RC el nuevo paradigma de la "diligencia debida" se encuentre en otras normas europeas como el Reglamento de servicios digitales, el cual alude a las obligaciones de diligencia de las plataformas para crear un entorno en línea transparente y seguro (artículos 11 y ss), o la Propuesta de Directiva en relación con la obligación de diligencia debida de las empresas en materia de sostenibilidad".

24 Para MARTÍN CASALS, M. (2023). "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *op. cit.,* p. 73 "no se trata aquí de permitir al juez utilizar un estándar de prueba reducido ("razonablemente probable", parecido al *more probable than not* angloamericano) -que en nuestra doctrina a menudo se confunde con la "causalidad probabilística" (*proportional liability*), con la que nada tiene que ver-, sino de permitirle presumir el nexo causal entre la actuación culposa y la información o falta de información del sistema de IA en atención a las circunstancias del caso".

Por su parte, NAVAS NAVARRO, S. (2022). "Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial", *op. cit.,* p. 39 precisa que "el juez o tribunal podrá acudir a la norma sobre distribución dinámica de la prueba (artículo 217.7 de la LEC), a la conocida regla *res ipsa loquitur* o a presunciones de hecho a efectos de decidir el caso".

25 Vid., NAVAS NAVARRO, S. (2022). "Régimen *europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial", op.* cit., pp. 35-39; MARTÍ GRAU, R. (2023). "Reflexiones acerca de la

Por otra parte, los apartados 2 y 3 del artículo 3 distinguen entre, por una parte, las demandas interpuestas contra el proveedor de un sistema de IA de alto riesgo o contra una persona sujeta a las obligaciones del proveedor conforme lo dispuesto en el RIA; y, por otra parte, las demandas interpuestas contra el usuario de dichos sistemas (respecto de los que ya no se contiene referencia en el RIA). A este respecto, sigue las disposiciones respectivas y las condiciones pertinentes del citado Reglamente de Inteligencia Artificial. En el caso de las demandas fundadas en el artículo 4, apartado 2 el cumplimiento por parte de los demandados de las obligaciones enumeradas en dicho apartado debe evaluarse también a la luz del sistema de gestión de riesgos y sus resultados, es decir, las medidas de gestión de riesgos, con arreglo al citado RIA.

En el supuesto de los sistemas de IA de alto riesgo, tal como se definen en el mencionado cuerpo legal, el artículo 4, apartado 4 establece una excepción a la presunción de causalidad cuando el demandado demuestre que el demandante puede acceder razonablemente a pruebas y conocimientos especializados suficientes para demostrar el nexo causal. Esta posibilidad puede incentivar a los demandados a cumplir sus obligaciones de exhibición, las medidas establecidas por el RIA para garantizar un alto nivel de transparencia de la IA o, los requisitos de documentación y registro que, establece el citado Reglamento. Además, esta relación de causalidad opera entre la información o falta de información de salida generada por un sistema de IA y el daño producido.

Ahora bien, teniendo en cuenta lo establecido en los capítulos II y III del RIA en cuanto a los requisitos y obligaciones que han de cumplir los sistemas de IA de alto riesgo, la culpa necesaria para que opere la relación de causalidad es la que deriva del incumplimiento de tales requisitos y obligaciones. En todo caso, la Propuesta de Directiva distingue entre los daños causados por los proveedores de dichos sistemas de IA de alto riesgo y los daños causados por los usuarios. Estos últimos, como hemos indicado, ya no se mencionan en el RIA, por lo que se prescinde de tal elemento subjetivo al no mencionarse como sujeto obligado.

De todas formas, el requisito relativo a la culpa solo se cumplirá cuando el demandante haya demostrado que el proveedor o, en su caso, la persona sujeta a las obligaciones del proveedor, ha incumplido los otros dos requisitos establecidos y mencionados en líneas precedente. Por lo que, el primer requisito relativo a la culpa permite presumir la relación de causalidad, si se dan los otros dos requisitos previstos en el artículo 4.1 letras b) y c). Así, podemos referirnos a las acciones que se entablen contra proveedores de sistemas de IA de alto riesgo que utilicen técnicas que implican el entrenamiento de modelos de datos, se presume la culpa y, por ende, la relación de causalidad si no se han desarrollado a partir de conjuntos de datos de entrenamiento, validación y prueba que cumple los requisito de calidad dispuesto en el artículo 17 del RIA; o también cuando, precisamente, el

Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños", *Revista Aranzadi Doctrina, número 4, abril*, p. 5.

sistema no se ha diseñado, ni desarrollado; de forma que, cumpla con los requisitos de transparencia e información contenidos en el artículo 13 del citado Reglamento; o cuando el sistema de IA no ha sido diseñado ni desarrollado, de modo que permita una vigilancia efectiva por las personas físicas durante el periodo de utilización del sistema de IA de conformidad con el artículo 14 del RIA; o, asimismo, cuando el sistema no ha sido diseñado ni desarrollado, de manera que, a la luz de su finalidad prevista, alcance el nivel adecuado, de precisión, solidez y ciberseguridad en virtud del artículo 15 del RIA; o, en fin, no se hayan adoptado de forma inmediata las medidas correctoras necesarias para poner el sistema de IA conforme las obligaciones establecidas en el capítulo III, sección 3ª del mencionado texto legal; o para retirar del mercado o recuperar en sistema según proceda, atendiendo a lo establecido en el artículo 20 del RIA.

En este contexto, aunque la Propuesta de Directiva se centra en la responsabilidad civil de los sistemas de IA de alto riesgo principalmente; cuando se trata de supuesto de sistemas de IA de no alto riesgo el artículo 4 apartado 5 establece una condición para la aplicabilidad de la presunción de causalidad en virtud de la cual esta última está sujeta a que el órgano jurisdiccional determine que, resulta excesivamente difícil para el demandante demostrar el nexo causal. Tales dificultades deben evaluarse a la luz de las características de determinados sistemas de IA, como la autonomía y la opacidad, que hacen muy difícil en la práctica la explicación del funcionamiento interno del sistema de IA[26]; lo que afecta negativamente a la capacidad del demandante para poder demostrar el nexo causal entre la culpa del demandado y la información de salida de IA[27].

En los casos en que el demandado utilice el sistema de IA en el transcurso de una actividad personal y no profesional, el artículo 4, apartado 6 dispone que la presunción de causalidad solo debe aplicarse, si el demandado ha interferido sustancialmente en las condiciones de funcionamiento del sistema de IA, o si el demandado tenía la obligación y estaba en el ámbito de determinar los requisitos de funcionamiento del sistema de IA y no lo hizo. Esta condición se justifica por la necesidad de ponderar los intereses de los perjudicados y de los usuarios no profesionales, eximiendo de la aplicación de la presunción de causalidad aquellos

26 MARTÍ GRAU, R. (2023). "Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños", *op. cit.*, p. 3 tras señalar que "la Propuesta de Directiva de IA no ofrece explicación alguna acerca del porqué de esta diferencia entre los sistemas de IA de alto riesgo y los que no lo son". A continuación acertadamente indica que "nada impide que en determinados supuestos, los sistemas de IA que no son de alto riesgo puedan ocasionar daños de más entidad que los sistemas de IA de alto riesgo".

27 Al respecto indica el considerando número 28 de la Propuesta de Directiva: *"(…) Los órganos jurisdiccionales nacionales deben aplicar la presunción cuando el demandante se encuentre en una situación excesivamente difícil para demostrar la causalidad por verse en la obligación de explicar la manera en que el acto u omisión humano determinante de la culpa llevó al sistema de IA a producir la información de salida que dio lugar al daño o a no producir la información de salida cuya ausencia dio lugar al daño. Sin embargo, no debe exigirse al demandante que explique las características del sistema de IA de que se trate ni el modo en que estas características dificultan la determinación del nexo causal".*

casos en que los usuarios no profesionales no incrementen el riesgo a través de su comportamiento.

Por último, el artículo 4 apartado 7 dispone que el demandado tiene derecho a refutar, esto es, desvirtuar la presunción de causalidad basada en el artículo 4, apartado 1 mediante prueba en contrario.

Ahora bien, procede indicar que, estas normas en materia de responsabilidad civil en el fondo tienen la ventaja adicional de ofrecer a todos los que participan en actividades relacionadas con sistemas de IA un incentivo adicional para cumplir sus obligaciones en relación con la conducta que se espera de ellos.

Sobre tales bases, reiteramos, de nuevo, que salvo en lo señalado respecto a las presunciones que establece, esta Propuesta de Directiva no armoniza con las legislaciones nacionales en lo relativo a la parte sobre la que recae la carga de la prueba o al grado de certeza necesario para que haya fuerza probatoria, ni con las condiciones relacionadas con los daños, esto es, la cuestión de qué daños son indemnizables, que también están regulados por la legislación nacional y de la Unión aplicable.

Ahora bien, para que se aplique la presunción de causalidad contenida en la Propuesta de Directiva, la culpa del demandado debe establecerse como una acción u omisión humana que no se ajuste a un deber de diligencia derivado del Derecho de la Unión o nacional directamente destinado a proteger contra los daños que se hayan producido. Así pues, esta presunción puede aplicarse, por ejemplo, en demandas de indemnización por lesiones corporales cuando el órgano jurisdiccional establezca la culpa del demandado por incumplimiento de las instrucciones de uso destinadas a evitar daños a personas físicas. El incumplimiento de deberes de diligencia no destinados directamente a proteger contra los daños producidos no da lugar a la aplicación de la presunción. De todas formas, debe ser necesario establecer que puede considerarse razonablemente probable, basándose en las circunstancias del caso, que la culpa haya influido en la información de salida producida por el sistema de IA o que el sistema de IA no haya producido una información de salida. Por último, debe exigirse al demandante que demuestre que la información de salida, o la no producción de información de salida, dio lugar al daño.

En todo caso, esta culpa puede establecerse en relación con el incumplimiento de las normas de la Unión que regulan específicamente los sistemas de IA de alto riesgo, como los requisitos introducidos para determinados sistemas de IA de alto riesgo el RIA y que puedan introducirse en una futura legislación sectorial para otros sistemas de IA de alto riesgo de conformidad con el artículo 2 del RIA o, en fin, a los deberes de diligencia vinculados a determinadas actividades y que son aplicables con independencia que la IA se utilice o no para esa actividad. Al mismo tiempo, esta Propuesta de Directiva ni crea, ni armoniza los requisitos o la responsabilidad de las entidades cuya actividad está regulada por dichos actos jurídicos y, por tanto, no da lugar a nuevas demandas de responsabilidad. La prueba

del incumplimiento de tales requisitos determinantes de la culpa se llevará a cabo de conformidad con las disposiciones de dichas normas aplicables del Derecho de la Unión, ya que esta Propuesta de Directiva no introduce nuevos requisitos, ni afecta a los vigentes. Así, la exención de responsabilidad de los prestadores de servicios intermediarios y las obligaciones de diligencia debida a las que están sujetos en virtud de la Ley de Servicios Digitales no se ven afectadas por esta Propuesta de Directiva. Del mismo modo, el cumplimiento de los requisitos impuestos a las plataformas en línea para evitar la comunicación no autorizada al público de obras protegidas por derechos de autor debe establecerse en virtud de la 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 otra legislación pertinente de la Unión en materia de derechos de autor.

Ahora bien, en los ámbitos no armonizados por el Derecho de la Unión, sigue siendo de aplicación el Derecho nacional y la existencia de culpa se determina en virtud de la legislación nacional aplicable. Todos los regímenes nacionales de responsabilidad establecen obligaciones de diligencia y adoptan como norma de conducta diferentes expresiones del principio relativo a actuar como una persona razonable; garantizando con ello también un funcionamiento seguro de los sistemas de IA y, por ende, evitando el menoscabo de los intereses jurídicos protegidos. Estos deberes de diligencia podrían, por ejemplo, exigir a los usuarios de sistemas de IA que elijan para determinadas tareas un sistema de IA concreto con características determinadas, o que excluyan a determinados segmentos de una población de la exposición a un sistema de IA concreto.

En fin, aun cuando se demuestre la existencia de una culpa consistente en el incumplimiento de un deber de diligencia destinado directamente a proteger contra los daños sufridos, no toda culpa debe dar lugar a la aplicación de la presunción refutable que la vincula a la información de salida de la IA. Tal presunción solo debe aplicarse cuando pueda considerarse razonablemente probable, en función de las circunstancias en que se produjo el daño, que dicha culpa ha influido en la información de salida producida por el sistema de IA, o en la no producción de la información de salida por parte del sistema de IA que haya dado lugar al daño.

Por otra parte, las características específicas de determinados sistemas de IA, como la autonomía y la opacidad pueden dificultar excesivamente al demandante la satisfacción de la carga de la prueba; así podrían darse situaciones en las que no se den tales dificultades por disponer el demandante de suficientes pruebas y conocimientos especializados para demostrar el nexo causal. Este podría ser el caso, por ejemplo, de los sistemas de IA de alto riesgo respecto de los cuales el demandante puede tener un acceso razonable a pruebas y conocimientos especializados suficientes mediante requisitos de documentación y registro de conformidad con el RIA. En tales situaciones, el órgano jurisdiccional no debe aplicar la presunción.

La aplicación de la presunción de causalidad tiene por objeto garantizar al perjudicado un nivel de protección similar al existente en aquellas situaciones en las que no interviene la IA y en las que, por tanto, la causalidad puede ser más fácil de demostrar.

Ahora bien, no olvidemos que, estamos operando con una presunción refutable (*iuris tantum*); de ahí que, el demandado debe tener la posibilidad de refutarla; en particular, demostrando que su culpa no puede haber sido la causa del daño.

7.4. Revisión y trasposición de la Propuesta de Directiva

Con respecto a la trasposición, el considerando número 32 de la Propuesta partiendo de la necesidad de realizar adaptaciones en las normas nacionales de responsabilidad civil y procesales con el fin de fomentar la introducción generalizada de productos y servicios basados en la IA en condiciones beneficiosas para el mercado interior, y, de procurar una aceptación social y, de confianza por parte de los consumidores en la tecnología de la IA y en el sistema judicial, conviene fijar un plazo máximo de entrada en vigor esta Directiva para que los Estados miembros adopten las medidas de transposición que resulten necesarias.

En cuanto a la revisión, el propio considerando número 31 señala que resulta necesario prever una revisión de la presente Directiva (cinco años) después de la finalización del período de transposición. En particular, en dicha revisión deberá examinarse si es necesario adoptar normas de responsabilidad objetiva (sin culpa) para las demandas contra el operador -siempre que estas no estén ya cubiertas por otras normas de responsabilidad de la Unión, en particular la Directiva 85/374/CE- combinadas con un seguro obligatorio para la explotación de determinados sistemas de IA, tal como ha sugerido, en varias ocasiones, el Parlamento Europeo.

Si bien, atendiendo al principio de proporcionalidad, procede evaluar dicha necesidad de revisión a la luz de la evolución tecnológica y normativa pertinente en los próximos años, teniendo en cuenta el efecto y la incidencia en la introducción generalizada y la adopción de los sistemas de IA, especialmente para las pymes.

8. BIBLIOGRAFÍA

ATIENZA NAVARRO, Mª.L. (2024). ¿Daños nuevos, reglas nuevas para su indemnización? Responsabilidad Civil e inteligencia artificial a la luz de las últimas propuestas de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías, número 64, enero-abril*, pp. 33-86.

BARRIO ANDRÉS, M. (2024). "Algunos claroscuros en el Reglamento Europea de Inteligencia Artificial", *Diario La Ley, núm. 86, sección ciberderecho, 30 de julio*, pp. 1-3.

- "Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial". En. M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia Artificial*, Valencia: Tirant lo Blanch.

CAMPOS ACUÑA, C. (2024). "Las 15 claves del Reglamento Europeo de IA (AI Act) (1)", *El Consultor de los Ayuntamientos, 15 de julio*, pp. 1-11.

DELGADO MARTÍN, J. (2024). "Notas sobre el uso de la IA generativa por profesionales de la justicia", *Diario La Ley, núm. 10568, sección tribuna, 16 de septiembre*, pp. 1-3.

FIERO RODRÍGUEZ, D. (2024). "Aplicaciones sobre la creación del Consejo Asesor Internacional de la Inteligencia Artificial", *Diario La Ley, núm. 86, sección ciberderecho, 2 de septiembre*, pp. 1-14.

MARTÍ GRAU, R. (2023). "Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños", *Revista Aranzadi Doctrina, número 4, abril*, pp. 1 a 11 (versión digital).

MARTÍN CASALS, M. (2023). "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causado por sistemas de Inteligencia Artificial", *Indret, núm. 3*, pp. 55-100.

MUÑOZ GARCÍA, C. (2024). "Modelos de Inteligencia Artificial de uso general y sistemas de riesgo limitado y mínimo". En. M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia Artificial*, Valencia: Tirant lo Blanch.

ORTIZ FERNÁNDEZ, M. (2024). "La "adaptación" del derecho de daños a la Inteligencia Artificial: la propuesta de Directiva sobre responsabilidad, *Revista de internet, derecho y política, número 40, marzo*, pp. 1 a 12.

NAVAS NAVARRO, S. (2022). "Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de Inteligencia Artificial, *Revista CESCO de derecho de Consumo, núm. 44*, pp. 27 a 51.