Sistemas de inteligencia artificial y prevención de los riesgos laborales. Obligaciones del proveedor y del empresario

Artificial intelligence systems and the prevention of occupational risks: obligations of the supplier and the employer

José Luis Goñi Sein
Catedrático de Derecho del Trabajo y Sseguridad Social
Universidad Pública de Navarra
ORCID ID: 0000-0003-4481-9483

doi: 10.20318/labos.2024.9036

Resumen: El propósito de este trabajo es analizar la interación existente entre el Reglamento UE de Inteligencia Artificial y la normativa de prevención de riesgos laborales, respecto de la utilización de los sistemas de IA en el ámbito laboral. Estas dos normativas presentan una identidad de razón en cuanto al enfoque basado en el riesgo y al objetivo, pues tratan de mitigar los potenciales riesgos, pero, al mismo tiempo, presentan diferencias notables sobre el alcance del riesgo, dando lugar a antinomias. Se trata de resolver estas antinomias, haciendo una interpretación integradora de los dos sistemas normativos y de sus finalidades, con el objeto de establecer el conjunto de obligaciones que deben tener en cuenta, tanto el proveedor de IA, como el responsable del despliegue (empresario) para su introducción en el mercado y su puesta en servicio, desde el punto de vista de la prevención de riesgos laborales.

Palabras clave: Inteligencia artificial, ámbito laboral, riesgos laborales, proveedor de IA, empresario, obligaciones preventivas.

Abstract: The purpose of this paper is to analyse the interplay between the EU Regulation on Artificial Intelligence and the EU regulation on occupational risk prevention with regard to the use of AI systems in the workplace. These two regulations present an identity of reason in terms of risk-based approach and objective, as they seek to mitigate potential risks, but, at the same time, they present notable differences on the scope of risk, giving rise to antinomies. The aim is to resolve these antinomies by making an integrative interpretation of the two regulatory systems and their purposes, in order to foresee which set of obligations must be taken into account, both by the AI provider and the person responsible for the deployment (employer) for its introduction in the market and its commissioning, from the point of view of occupational risk prevention.

Keywords: Artificial intelligence, work environment, occupational risks, AI provider, employer, preventive obligations.

1. Introducción

La IA aporta numerosos beneficios a la vida de los ciudadanos, también al ámbito de la seguridad y salud laboral, ayudando a identificar los peligros, "predecir riesgos potenciales, proporcionar monitoreo en tiempo real, reconocer comportamientos inseguros, detectar condiciones inseguras y sugerir formas de riesgos potenciales"[1]. Asimismo, resulta muy útil para conocer el estado de salud o mejorar la vigilancia de la salud del trabajador, evaluar el grado de malestar psicológico, o los posibles efectos negativos para la salud mental del trabajador, en particular, cuando está sometido a presión para alcanzar un determinado nivel de productividad. Mediante sistemas de gestión de personal basada en la IA cabe detectar el grado de estrés, el síndrome de desgaste profesional o y de agotamiento, de manera que se puedan adoptar medidas de prevención[2].

Pero no son las capacidades o beneficios de la IA el objeto de este análisis, sino los desafíos que para las personas y la sociedad presenta la incorporación de la IA al ámbito de las relaciones laborales, en concreto, a los equipos de trabajo y sistemas de gestión de recursos humanos. El desafío principal, dejando aparte los problemas jurídicos, o éticos, es que los sistemas de IA o las máquinas u ordenadores que incorporen dichos sistemas, no funcionen correctamente o sencillamente generen riesgos, convirtiéndose en daños en el mundo laboral para la seguridad y salud laboral, incluyendo los riesgos psicosociales. Y ello no solo como consecuencia de errores en el diseño y fabricación de los sistemas de IA, porque pueden contener "errores significativos y alucinaciones debidas a circunstancias multifactoriales como la desactualización de los datos de entrenamiento, fallos informáticos, intereses comerciales, sesgos por género, raza y contextos sociales"[3], sino porque sus actos resultan menos predecibles en virtud de que pueden actuar y perseguir objetivos de forma autónoma.

La identificación y el control de esos riesgos para los derechos, la seguridad y el buen funcionamiento del mercado único de la Unión Europea constituyen el punto central y una de las aristas más complejas de la IA. La determinación del riesgo es el *prius* que condiciona los parámetros, bien de uso inaceptable o de uso legítimo del sistema

[1] Vid. EU-OSHA: El impacto de la Inteligencia Artificial en la Seguridad y Salud en el trabajo". Disponible en: https://osha.europa.eu/es/publications/impact-artificial-intelligence-occupational-safety-and-health.

Gracias a la creciente disponibilidad de datos y macrodatos (big data) y a la capacidad de usar algoritmos para el tratamiento de datos, los sistemas de IA permiten monitorear continuamente los parámetros de las máquinas y los entornos de trabajo, lo que ayuda a reducir el riesgo de errores mecánicos y humanos. Los sistemas de IA "pueden entrenarse para detectar peligros de seguridad que los humanos tal vez no puedan ver, como grietas microscópicas en una estructura o cambios sutiles en los vitales de un paciente" vid. ABDULLAH MALIK: *Artificial Intelligence in Health and Safety*, 22 de febrero de 2023 Disponible en: https://safetypedia-com.translate.goog/safety/artificial-intelligence-in-health-and-safety/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc.

[2] Sobre dispositivos inteligentes para la seguridad y salud en el trabajo, vid. LLORENS ESPADA, J.*: Límites al uso de la Inteligencia Artificial en el ámbito de la salud*, La Ley, Madrid, 2023, pp. 151 y ss.

[3] VESTRI, G.: "La Unión Europea estrena el Reglamento de Inteligencia Artificial (RIA).Control, supervisión y uso de una tecnología cada vez más presente en la vida de todos", *Diario LA LEY*, Nº 10550, 19 de Julio de 2024.

de IA, porque se quiere que la IA sea desarrollada y utilizada de manera segura, ética y respetuosa con los Derechos fundamentales y los valores fundacionales de la Unión Europea Las obligaciones impuestas a los proveedores o usuarios vendrán determinadas en función de los riesgos concretos que comporta el uso de la IA.

Pero la noción de riesgo que se toma en consideración en este estudio es un riesgo algo más concreto, está relacionada con la seguridad y la salud de la persona del trabajador en el ámbito de la relación laboral. La perspectiva que aquí interesa es la de los riesgos conocidos y razonablemente previsibles de los sistemas de IA para la salud, la seguridad de los trabajadores (dejando fuera los relativos a los derechos fundamentales), teniendo en cuenta su finalidad prevista y también su uso indebido razonablemente previsible, así como los posibles riesgos derivados de la interacción entre el sistema de IA y el entorno en el que opera.

En la línea de lo señalado, el Reglamento (UE) de Inteligencia Artificial (RIA)[4] promueve un enfoque europeo de la IA centrado en el riesgo y tiene por objeto garantizar la protección de los derechos fundamentales y la seguridad de los usuarios en los ámbitos de especial incidencia. Uno de los ámbitos de alto riesgo predefinidos en el RIA (Anexo III) es la relación laboral en el que uno de los usuarios importantes o grupos de usuarios que se espera que interactúen o aprovechen la IA, es la empresa y, a la vez, el trabajador, que desarrolla su actividad laboral expuesto, no solamente a los riesgos específicos del puesto de trabajo, sino a los derivados de la IA.

El acercamiento al problema de los riesgos laborales de la IA no puede ser realizado, basándose simplemente en los enunciados de la normativa de la IA, porque en realidad el RIA no se ocupa de este tema. Aborda los riesgos de la IA de manera genérica, prohibiendo o limitando el uso de sistemas de IA que presenten un riesgo inaceptable para la seguridad, la salud, la dignidad o la autonomía de las personas, o que violen los valores democráticos. No obstante, las normas armonizadas que se establecen en el RIA deben entenderse -según indica el Considerando 9- 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.

La aproximación al tema preventivo laboral del RIA requiere, por tanto, un enfoque conjunto, en el que se tome en consideración el orden jurídico laboral, en particular,

[4] El día 12 de julio de 2024 el RIA se publicó en el Diario Oficial de la Unión Europea el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial o AI Act), en lo sucesivo RIA o el Reglamento simplemente), que entró en vigor el 1 de agosto de 2024, aunque su aplicación se producirá de forma diferida. Será aplicable a partir del 2 de agosto de 2026. No obstante: a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025; b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101; c) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

el marco preventivo laboral, porque, como se advierte en el Considerando 9, el RIA no debe afectar al Derecho de la Unión en materia de política social ni a la legislación laboral nacional —conforme al 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.

Ahora bien, en seguida surgen las fricciones porque la conceptuación del riesgo de la normativa de IA y la de la normativa de prevención de riesgos laborales divergen notablemente. Como se verá, la regulación de la IA atiende a la magnitud del riesgo y a criterios extrasistemáticos de matriz económica, pues, aparte de prever una clasificación de los sistemas de IA según el nivel de riesgo, busca promover la innovación y la competitividad en el sector de la IA, procurando no obstaculizar el desarrollo económico[5]. En cambio, el concepto de riesgo recabado de la normativa de seguridad y salud laboral no establece categorización alguna y se basa únicamente en la protección de vida y la seguridad y salud de la persona del trabajador.

Aquí se trata de conectar ambas soluciones valorativas, de integrar el complejo entramado de principios de los dos ordenamientos jurídicos concurrentes, y de extraer criterios racionales para alcanzar un punto de equilibrio entre los dos sistemas de protección de riesgo, viendo qué obligaciones deben observar los proveedores y cuáles los desarrolladores de los sistemas de IA (empresarios) a partir de los requisitos del RIA y los específicos de prevención de los riesgos laborales.

2. La noción de riesgo protegido en la LPRL

Antes de adentrarnos en la conceptualización del riesgo en el RIA, procede exponer sucintamente el significado y alcance de riesgo laboral y su prevención en el ámbito del ordenamiento jurídico laboral, pues, al contrario de lo que somos inducidos a creer por la modernidad de la materia regulada, no se antepone el marco normativo regulador de la IA por ser la norma posterior, sino que, al contrario debe prevalecer la normativa de prevención laboral porque, como se ha señalado, la nueva normativa de protección en materia de IA viene a complementar la normativa de prevención de riesgos laborales y no al revés.

Es importante subrayar esto, ya que la normativa laboral preventiva no debe doblegarse al servicio de los objetivos de la IA, sino que ésta debe interpretarse a la luz de las irreductibles especificidades de aquella. Y ello porque la normativa de IA ha de tratar

[5] Considerando 8: "*En consecuencia, se necesita un marco jurídico de la Unión que establezca unas normas armonizadas en materia de IA para impulsar el desarrollo, la utilización y la adopción en el mercado interior de la IA y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, en particular la democracia, el Estado de Derecho y la protección del medio ambiente, reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado, la puesta en servicio y la utilización de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de libre circulación de mercancías y servicios*".

de conectarse con otros modelos de regulación vigente en esta materia o en otras como la de seguridad del producto.

Como pone de manifiesto el Considerando 64, los peligros de los sistemas de IA abarcados por los requisitos del Reglamento IA "*se refieren a aspectos diferentes de los contemplados en los actos de armonización de la Unión existentes*" y, por consiguiente, los requisitos del Reglamento IA "*completa*(n) *el conjunto existente de actos de armonización de la Unión*". Por ejemplo, se señala que las máquinas 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 pertinente de la Unión, ya que esa legislación sectorial no aborda los riesgos específicos de los sistemas de IA.

Así las cosas, es preciso conocer el contexto en el que debe ser aplicada la nueva normativa europea en materia de IA. En este sentido, cabe recordar, aunque sea un lugar común, que la normativa general de prevención de riesgos laborales (la Directiva 89/391//CEE, relativa a la aplicación de medidas para promover la mejora de la seguridad y salud de los trabajadores), y la norma de trasposición a nuestro ordenamiento (la LPRL), imponen un deber empresarial de garantizar la seguridad y salud de los trabajadores frente a los riesgos laborales.

La normativa de prevención de riesgos laborales concibe el "riesgo laboral" como *la posibilidad de que un trabajador sufra un determinado daño derivado del trabajo* (art. 4.2 LPRL). Dicha normativa tiene por objeto identificar y estimar la magnitud del riesgo para posteriormente evitarlo o, en su caso, reducirlo y controlarlo. Entre los principios generales que integran el deber general de prevención laboral (art. 15.1 LPRL), se hallan los de: a) evitar los riesgos; b) evaluar los riesgos que no se puedan evitar; c) combatir los riesgos en su origen.

La LPRL establece un criterio general de protección de la seguridad y salud laboral del trabajador, sin excluir, ni distinguir ningún tipo de riesgo. Considera que, para calificar un riesgo desde el punto de vista de su gravedad, se debe atender conjuntamente a la probabilidad de que se produzca el daño y a la severidad del mismo (art. 4.2 LPRL).

El empresario contrae con el trabajador una deuda de seguridad, que no se satisface con el mero cumplimiento formal de la normativa en materia de prevención de riesgos laborales. El empresario está obligado a adoptar cuantas medidas sean necesarias para evitar el daño, desarrollando una acción permanente de seguimiento de la actividad preventiva, identificando, evaluando y controlando los riesgos que no se hayan podido evitar, y de los niveles de protección (art. 14.2 LPRL).

La deuda de seguridad requiere una diligencia constante por parte del empleador para evitar que el daño se produzca. Incumbe al empleador proteger al trabajador incluso frente a sus propias imprudencias profesionales. Por ello, entre las medidas preventivas que debe adoptar se incluye la de prever las distracciones o imprudencias no temerarias que el empleador pudiera cometer en el desarrollo de su actividad laboral (art. 15.4 LPRL).

El empresario, para evitar la responsabilidad, ha de acreditar haber agotado toda diligencia posible incluso más allá de las exigencias reglamentarias. Solo queda exonerado de responsabilidad si el resultado lesivo se hubiese producido por fuerza mayor o caso

fortuito, por negligencia exclusiva no previsible del trabajador o por culpa exclusiva de terceros no evitable por el empresario. Aun y todo, corresponde al empresario acreditar la concurrencia de esa posible causa de exoneración, en tanto que él es el titular de la deuda de seguridad y habida cuenta de los términos cuasiobjetivos en que la misma está concebida legalmente [STS (Sala 4ª) 30 de junio de 2010, R. 4123/2008].

3. La noción de riesgo en el RIA

La normativa de IA comparte elementos con la normativa de prevención de riesgos laborales: por un lado, sitúa el centro de gravedad en la valoración del riesgo[6], que es inherente a cualquier actividad social o económica; y, por otro, persigue como objetivo controlar el riesgo.

En efecto, tal como se ha señalado, el RIA ha sido diseñado con un enfoque basado en el riesgo. El sistema de protección frente a los perjuicios que conlleva el uso de los medios y sistemas de IA se construye sobre la noción de riesgo para los derechos, la seguridad y el buen funcionamiento del mercado único del Unión Europea. El riesgo se define como "*la combinación de la probabilidad de que se produzca un daño y la gravedad del daño*" (art. 3.2 RIA). De forma que, el concepto de daño o perjuicio se erige en la piedra angular sobre el que se asienta el riesgo.

Por otra parte, el RIA persigue el mismo objeto que la LPRL, porque trata de identificar y estimar la magnitud del riesgo para posteriormente evitarlo o, en su caso, reducirlo y controlarlo. El RIA impone a los proveedores obligaciones orientadas a evaluar riesgos concretos y a aplicar medidas de reducción del riesgo razonable. Su control constituye, por tanto, el objetivo clave de la actividad preventiva.

No obstante, ambas legislaciones presentan, algunas diferencias importantes:

3.1. La categorización del riesgo en el RIA: distinción entre riesgo sistémico y riesgo crónico

Difieren sobre la categorización de riesgo. La LPRL establece un criterio general, sin excluir, ni distinguir ningún tipo de riesgo. Considera, como se ha observado, que, para calificar un riesgo desde el punto de vista de su gravedad, se debe atender conjuntamente a la probabilidad de que se produzca el daño y a la severidad del mismo (art. 4.2 LPRL).

Sin embargo, de acuerdo con la propia configuración del RIA, es preciso distinguir entre dos grandes categorías: por un lado, los riesgos extremos o sistémicos, seguramente de muy reducida probabilidad en el ámbito laboral, pero de una intensidad e implicaciones mucho más graves; y, por otro lado, los riesgos crónicos de alta frecuencia pero de intensidad moderada.

[6] MERCADER UGUINA, J.: "Los usos de alto riesgo en el ámbito laboral de la IA y la certificación", *El Foro de Labos, 9/5/2024*, Disponible en: https://www.elforodelabos.es/2024/05/los-usos-de-alto-riesgo-en-el-ambito-laboral-de-la-ia-y-la-autocertificacion/

Inicialmente la Propuesta de Reglamento de IA solo contemplaba los riesgos crónicos, pero en su proceso normativo de elaboración, especialmente su fase final, a consecuencia de la aparición de los denominados GPAI, (los General Purpose AI sistems and models) se ha insertado una regulación de los modelos y sistemas de IA de uso general[7].

Los riegos extremos abarcarían los modelos de sistemas de IA general, que, por el incremento de capacidades y la autonomía de estos sistemas, "podrían amplificar el impacto de la IA, planteando unos riesgos que incluyen daños sociales a gran escala, usos maliciosos y una pérdida irreversible del control humano sobre los sistemas autónomos de IA"[8].

Se incluiría en esta categoría el llamado «riesgo sistémico», que el art. 3. 65 RIA, describe como "*un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor*"[9]. Este riesgo lo presentan aquellos productos elaborados con IA de aparición no tan frecuente en el lugar de trabajo, pero de posibles efectos devastadores para la seguridad y salud de las personas e integridad de los bienes.

Un modelo de IA de uso general se considerará que es de riesgo sistémico si reúne alguna de las siguientes condiciones:

a) tener capacidades de gran impacto evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia: se presumirá que un modelo de IA de uso general tiene las referidas capacidades de gran impacto cuando la cantidad acumulada de cálculo utilizada para su entrenamiento, medida en operaciones de coma flotante, sea superior a 1025) (art. 51.2 RIA).

---

[7] BARRIO ANDRÉS, M. : "Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial", *Diario LA LEY, Nº 86, Sección Ciberderecho*, 30 de Julio de 2024.

[8] Parafraseando al grupo de expertos del documento AA. VV.: "Managing extreme AI risks amid rapid progress", *Science* , 20 may 2024, Vol. 384: https://www.science.org/doi/10.1126/science.adn0117

[9] Considerando 110: "*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, en particular 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*".

b) tener, con arreglo a una decisión de la Comisión, adoptada de oficio o a raíz de una alerta cualificada del grupo de expertos científicos, las capacidades o un impacto equivalente a los establecidos en la letra a), de acuerdo con los criterios establecidos en el anexo XIII[10] (art. 51.1 RIA).

No obstante, la Comisión Europea puede modificar los referidos umbrales para clasificar los modelos de IA de uso general —los modelos GPAI— como de riesgo «sistémico» en función de los avances tecnológicos, como las mejoras algorítmicas o la mayor eficiencia del hardware, cuando sea necesario, para que los umbrales reflejen el estado actual de la técnica (arts. 51.3 y 52.4 RIA). En consecuencia, la Comisión tiene 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[11].

Dentro de la segunda categoría llamada de "riesgos crónicos" cabe considerar los sistemas de IA del Anexo III de efectos mucho más moderados. En el marco conceptual del RIA, el riesgo crónico se construye sobre una escala de riesgos en función de la capacidad para inferir daños para las personas y la sociedad y vulneraciones a derechos fundamentales. Se trata de un riesgo relacionado con la puesta en marcha y uso de determinados sistemas de IA que deberán cumplir los estándares del RIA para poder operar en Europa y de esta manera, quizá de forma indirecta, proteger a los ciudadanos europeos[12].

---

[10] ANEXO XIII: "*Criterios para la clasificación de los modelos de IA de uso general con riesgo sistémico a que se refiere el artículo 51:*

Con el fin de determinar si un modelo de IA de uso general tiene unas capacidades o unos efectos equivalentes a los contemplados en el artículo 51, apartado 1, letra a), la Comisión tendrá en cuenta los siguientes criterios:

a) el número de parámetros del modelo;

b) la calidad o el tamaño del conjunto de datos, por ejemplo medidos a través de criptofichas;

c) la cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo;

d) las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas);

e) los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso;

f) si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la Unión;

g) el número de usuarios finales registrados".

[11] BARRIO ANDRÉS, M. : "Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial", op cit.

[12] VESTRI, G.: "La Unión Europea estrena el Reglamento de Inteligencia Artificial (RIA). Control, supervisión y uso de una tecnología cada vez más presente en la vida de todos", op. cit.

3.2. La pirámide de riesgos crónicos

En el llamado riesgo crónico, el RIA establece una clasificación, dando lugar a lo que venimos calificando como una "pirámide de riesgos"[13] integrado por cuatro diferentes niveles de riesgo: inaceptable, alto, limitado y mínimo. En la base se sitúa el riesgo mínimo por su menor capacidad para generar daños, y en el nivel más alto el riesgo inaceptable o prohibido por ser contrario a los valores de la Unión. Y en sendos escalones intermedios se sitúan los sistemas de riesgo alto y los de riesgo medio.

El RIA incorpora, en el artículo 5, una serie de prácticas sobre las que extenderá un total veto a su introducción en el mercado, puesta en servicio o utilización. Se consideran como tales los sistemas de IA que integren técnicas deliberadamente manipuladoras o engañosas, así como técnicas subliminales que trasciendan la consciencia [art. 5.1. a) RIA]; aquellos que exploten "alguna de las vulnerabilidades de una persona o un grupo específico de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con el objetivo o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho grupo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra" [art. 5.1 b) RIA]; sistemas de IA que permitan "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" (esto es, la asignación de la conocida como "puntuación social" ("social scoring") por parte de las autoridades públicas) [art. 5.1.c) RIA]; "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" [art. 5.1.e) RIA]; "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" [art. 5.1.f) RIA]; "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" [art. 5.1.g) RIA]; "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" [art. 5.1.h) RIA].

En un segundo nivel, el RIA sitúa los sistemas calificados de alto riesgo, regulados en el art. 6 y ss, que "constituyen el verdadero núcleo principal de la regulación europea de la IA", a los que dedica la mayor parte de su contenido. Los sistemas de IA, que el RIA califica

[13] GOÑI SEIN, J. L.: "El Reglamento UE de Inteligencia Artificial y su interrelación con la normativa de seguridad y salud en el trabajo", AA. VV. (Dirs. EGUSQUIZA, M. A.; RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades*, Tirant lo Blanch, Valencia 2023, p. 83.

de alto riesgo[14], se definen por dos rasgos (Considerando 46 y art. 6.1 y 2 RIA): 1) porque "*la introducción en el mercado de la Unión, la puesta en servicio o la utilización de sistemas de IA de alto riesgo debe supeditarse al cumplimiento de determinados requisitos obligatorios* antes de su comercialización (sistema de gestión de riesgos, calidad de datos, transparencia, supervisión humana); y 2) porque sus efectos perjudiciales no deben entrañar "*riesgos inaceptables para intereses públicos importantes de la UE, reconocidos y protegidos por el Derecho de la Unión*".

Se reconoce abiertamente que los sistemas de IA de alto riesgo " *pueden tener un efecto adverso para la salud y la seguridad de las personas, en particular cuando funcionan como componentes de seguridad de productos*" (Considerando 47), es decir, que se caracterizan por conllevar un grado importante de efectos perjudiciales, pero sin llegar al grado de "inaceptables"; o sea, sin alcanzar la magnitud de las consecuencias adversas de las prácticas prohibidas en el art. 5 RIA.

En el marco conceptual del RIA, el alto riesgo se refiere a unos ámbitos predefinidos especificados en el Anexo III del Reglamento de IA. No obstante, la Comisión Europea está facultada para añadir, modificar o suprimir los casos de uso de los sistemas de IA de alto riesgo del Anexo III (art. 7, apartados 1 y 3, RIA) y para modificar o añadir nuevas condiciones en las que los sistemas de IA de alto riesgo del Anexo III no se considerarán de alto riesgo con arreglo al artículo 6.3 del RIA (art. 6, apartados 6 y 7, RIA). Al llevarlo a cabo, la Comisión debe sopesar explícitamente los beneficios económicos y sociales de los sistemas de IA frente a los riesgos, basándose en pruebas empíricas suficientes[15].

En un tercer nivel el RIA contempla los sistemas de IA que representan un Riesgo limitado. Son sistemas de IA que pueden influir en los Derechos o la voluntad de los usuarios, pero en menor medida que los sistemas de alto riesgo. Estos sistemas están sujetos a requisitos de transparencia o información. En concreto: en los sistemas de IA diseñados para interactuar con personas (chatbots) se debe informar de que se está tratando con un sistema de IA; en los sistemas de IA, incluidos los sistemas de uso general, se garantizará que los resultados del sistema de IA estén marcados en un formato legible por máquina y detectable como generado o manipulado artificialmente; en sistemas de reconocimiento de emociones y sistemas de clasificación biométrica se deberá informar de que se están usando; en los sistemas que generen o manipulen imágenes o audio de personas (ultrafalsificación) se deberá informar de que se trata de imágenes o sonidos

[14] Según el art. 6.1 RIA, *un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:*

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

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

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

[15] BARRIO ANDRÉS, M. : "Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial", op cit.

manipulados artificialmente. Existe el derecho a saber que se está hablando con un bot (en lugar de un humano) y que una imagen es creada o modificada por IA.

En último lugar, se menciona el Riesgo mínimo o bajo, que integra a los sistemas de IA que no tienen impacto directo en los Derechos fundamentales o la seguridad de las personas, y que ofrecen amplias opciones y control a los usuarios. Estos sistemas están libres de cualquier obligación normativa, para fomentar la innovación y la experimentación. Se alude, en concreto, a los sistemas de IA utilizados para fines lúdicos (como videojuegos) o puramente estéticos (como filtros fotográficos)[16]. Los fabricantes pueden acogerse voluntariamente al RIA, aplicando alguno o todos los requisitos establecidos en el capítulo III, sección 2 para los sistemas de alto riesgo, o adherirse a códigos de conducta para una IA confiable, que los contemplen, elaborados por ellos o por las organizaciones a las que pertenecen (art. 95 RIA).

3.3. Ámbitos de riesgo crónico predefinidos con relación al ámbito laboral

La clasificación de los sistemas de IA según el nivel de riesgo, presenta algunas prácticas que tienen su ámbito de proyección natural en la relación laboral.

En las prácticas prohibidas, como ya se ha señalado, queda proscrito el "uso de sistemas de IA para inferir las emociones[17] de una persona física en los lugares de trabajo (…), excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad [art. 5.1.f) RIA]. De este modo, "quedan vetadas las cada vez más frecuentes técnicas o métodos de análisis de aptitudes, habilidades y capacidades psicosociales de los procesos selectivos de las empresas cuando se integren, por ejemplo, valiéndose de las destrezas de los nuevos softwares utilizados en las entrevistas virtuales, sistemas para inferir las emociones y crear con ello un perfil psicotécnico de los candidatos, o detectar el estado emocional de éste a lo largo de la entrevista"[18].

En este sentido, caerían dentro de lo ilícito "los sistemas de IA integrados en *wereables* o plataformas de gestión laboral que procuren inferir información sobre estos estados

[16] VESTRI, G.: "La Unión Europea estrena el Reglamento de Inteligencia Artificial (RIA). Control, supervisión y uso de una tecnología cada vez más presente en la vida de todos", op. cit

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

[18] GOÑI SEIN,J.L.; RODRÍGUEZ SANZ DE GALDEANO, B.; LLORENS ESPADA, J.; MARIN MALO, M.: "El impacto del nuevo marco normativo europeo de la inteligencia artificial en las relaciones laborales", AA VV (Dir. RICHARD GONZÁLEZ, M.), en prensa edit J B. Bosch,

de ánimo o emociones de los trabajadores, valiéndose de cualquier medio como pudieran ser sensores biométricos, señales fisiológicas tales como la temperatura corporal, frecuencia cardíaca, resistencia de la piel y onda del pulso , reconocimiento facial , voz o incluso el procesamiento de datos que incluyan conductas del trabajador de las que pueda inferirse el estado de ánimo, como por ejemplo el uso concreto que se hace del smartphone"[19].

En cambio, sí podrán tener cabida aquellos dispositivos que, habiendo sido previstos como una medida integrada en el Plan de prevención de riesgos laborales, busquen detectar el estado físico del trabajador con el objeto de prevenir futuros accidentes de trabajo, o su utilización responda a objetivos médicos. Esto genera que estas técnicas deban someterse al bloque normativo de vigilancia de la salud laboral ex art. 22 LPRL como cualquier otro reconocimiento médico de salud laboral[20].

Con relación a los sistemas de alto riesgo (art. 6.2 RIA), las actividades de IA que tienen una directa proyección en el ámbito laboral, se encuentran especificados en el punto 4 del Anexo III. En concreto, se consideran como de alto riesgo los que afecten al "*empleo, gestión de los trabajadores y acceso al autoempleo*", en particular, a) "*Sistemas de IA destinados a ser utilizados para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos", y " b) sistemas de IA destinados a utilizarse para tomar decisiones o influir sustancialmente en ellas que afecten a la iniciación, promoción y resolución de relaciones contractuales de índole laboral, a la asignación de tareas basada en la conducta individual o en rasgos o características personales, o al seguimiento y evaluación del rendimiento y la conducta de la personas en el marco de dichas relaciones*".

Se comprueba fácilmente que el Anexo III no constituye una relación acabada de potenciales ámbitos de alto riesgo derivados de sistemas de IA utilizados en el ámbito laboral, sino una relación más bien indicativa. En el ámbito laboral predefinido por el RIA, la mayor parte de actividades enumeradas constituyen gestión de recursos humanos. Pero puede haber también otros sistemas de IA no catalogados como de alto riesgo que podrían tener dicha consideración en atención a los riesgos que entrañan, como, por ejemplo, los sistemas de IA incorporados a máquinas con funciones de eficiencia o seguridad de bienes y personas, o, en materia preventiva, los equipos de protección individual inteligentes, o las plataformas digitales para la gestión de la PRL, y en general cualquier plataforma 4.0 que integre "innovaciones tecnológicas, como sistemas cognitivos, que son implementados a través de la aplicación de la Inteligencia Artificial a los datos, redes neuronales convolucionales (CNN) y aprendizaje por refuerzo profundo (DRL), haciendo que sean capaces de controlar un enorme conjunto de parámetros relacionados con procesos y el entorno"[21].

---

[19] Idem

[20] Idem

[21] LLORENS ESPADA, J.: "Inteligencia artificial y salud laboral", AA. VV. (Dirs. EGUSQUIZA, M. A.; RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades*, Tirant lo Blanch, Valencia 2023, p. 221.

Desde la perspectiva del marco normativo de prevención de riesgos laborales, conviene tener presente la distinta valoración de la relevancia del riesgo. A diferencia del RIA que fragmenta y limita el riesgo tomado en consideración, en la LPRL el "riesgo laboral" se concibe de manera íntegra y unitaria como la posibilidad de que un trabajador sufra un determinado daño derivado del trabajo (art. 4.2 LPRL) sin impropias distinciones. Lo que obliga al empresario a prever cualquier riesgo, en cualquier ámbito que se produzca, y con independencia de la gravedad.

De ahí que, el RIA advierta, en el Considerando (63), que "(e)l *hecho de que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea legal con arreglo a otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión*", añadiendo que 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*".

Ello nos lleva a afirmar, en línea de lo observado anteriormente, que la regulación de los sistemas de riesgo alto no se agota en sus propios requisitos, sino que conlleva una ulterior tarea de aplicación de los requisitos de Derecho derivado de la Unión y del Derecho nacional, en particular, respecto de la materia de prevención laboral, la Directiva 89/391 CEE, Directiva marco sobre salud y seguridad en el trabajo, de 12 de junio de 1989[22], y la LPRL.

A ello debe añadirse, además, que la vinculación del RIA exclusivamente a los sistemas de IA clasificados como de alto riesgo, no significa que, respecto del resto de los sistemas de IA no calificados como tal, no rija la normativa de prevención de riesgos laborales y, por tanto, no se aplique el deber del empresario de protección de los trabajadores frente a los posibles riesgos. La obligación del empresario de garantizar la seguridad y salud laboral, y de extremar la vigilancia en el cumplimiento de las normas de seguridad, es un principio de las relaciones laborales, que se aplica por igual a cualquier sistema de IA que entrañe cualquier tipo de riesgo laboral.

3.4. La valoración del riesgo: criterios de matriz económica

En el RIA se observa, aparte, un segundo elemento diferenciador con respecto a la LPRL, pues el RIA ha incorporado criterios extrasistemáticos de matriz económica, en la determinación del riesgo protegido. Conviene no olvidar que el RIA se propone crear un mercado único para la IA, facilitando la libre circulación y el reconocimiento de los sistemas de IA que cumplan con las normas de la UE. Lo cual obliga al intérprete a tener en cuenta inevitablemente en el horizonte hermenéutico del RIA valoraciones de política

[22] Pese a no estar incluida en la "Lista de actos legislativos de armonización de la Unión" del Anexo I, que en esta materia, tan solo menciona el Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a los equipos de protección individual y por el que se deroga la Directiva 89/686/CEE del Consejo (DO L 81 de 31.3.2016, p. 51)

de derecho, señaladamente, económicas, de comercio internacional y de funcionamiento de mercado

Esas consideraciones de orden económico no se aplican a los modelos de IA de uso general que pueden plantear los riesgos sistémicos, provocando, 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*" (Considerando 110), sino a los riesgos crónicos o menores.

Con respecto a la categoría de alto riesgo del Anexo III, de efectos mucho más moderados, el RIA incorpora matices importantes y algunos criterios limitativos de política de derecho que le alejan mucho, del ordenamiento jurídico laboral preventivo.

El riesgo tomado en consideración se contrae, por lo pronto, a los sistemas de IA que presentan un "riesgo considerable" 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" (Considerando 52). En este sentido, precisa el Considerando 53, que "es importante aclarar que pueden existir casos específicos en los que los sistemas de IA relativos a ámbitos predefinidos especificados en el presente Reglamento no entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por dichos ámbitos, dado que no influyen sustancialmente en la toma de decisiones o no perjudican dichos intereses sustancialmente". Es decir que, dentro de estos últimos, el sistema de obligaciones y garantías de RIA se extiende solo a aquellos que entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por dichos ámbitos, excluyendo a los que no influyen sustancialmente en la toma de decisiones o no perjudican dichos intereses sustancialmente (Considerando 53).

Pero ahí no acaba todo, porque el RIA restringe, aun más, los sistemas de IA sujetos al régimen obligacional del RIA, al obligar a tener en cuenta, además, valoraciones de política de derecho, y, más en concreto, valoraciones económicas de comercio internacional. Abiertamente se dispone en el Considerando (46) que: "*A fin de garantizar la coherencia y evitar una carga administrativa innecesaria o costes innecesarios, los proveedores de un producto que contenga uno o varios sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento o de los actos legislativos de armonización de la Unión enumerados en un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas relativas a la manera de garantizar la conformidad de un producto que contenga uno o varios sistemas de IA con todos los requisitos aplicables de la legislación de armonización de la Unión de manera óptima. La clasificación de un sistema de IA como «de alto riesgo» debe limitarse a aquellos sistemas de IA que tengan un efecto perjudicial importante en la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación reduce al mínimo cualquier posible restricción del comercio internacional*".

A la vista de lo cual, el intérprete tiene que introducir inevitablemente en el horizonte hermenéutico del RIA valoraciones de política de derecho, señaladamente, económicas, de comercio internacional y de funcionamiento de mercado. Criterios que obvia-

mente el interprete de la normativa de prevención laboral debe excluir por considerarlos ajenos a los únicos intereses en juego de la preservación de la seguridad y salud laboral del trabajador.

Parece que la "calificación 'de alto riesgo' "se limita a aquellos sistemas de IA que tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión", y debiendo además, reducirse "al mínimo cualquier posible restricción del comercio internacional, si la hubiera". Siendo así, se adopta una idea de alto riesgo bastante restrictiva, donde el objetivo de la seguridad y salud se subordina de alguna manera a las consideraciones económicas de no imponer restricciones innecesarias al comercio y de comprometer el desarrollo del mercado único.

En suma, la calificación de alto riesgo del sistema de IA dependerá del contexto de su específico de acuerdo con los criterios establecidos en el art. 6.3 RIA y los elementos interpretativos expuestos en los Considerandos 52 y 53 del RIA[23].

Ello tendrá, como ya he comentado en un anterior trabajo[24], un doble efecto significativo sobre la aplicación de los sistemas de IA en el lugar de trabajo, quedando probablemente excluidos buena parte de aquellos sistemas de IA. En primer lugar, porque no representen un efecto nocivo grave o alto sobre los trabajadores; de forma que, respecto de estos sistemas de IA, aunque representen un peligro para los trabajadores, no será necesario el cumplimiento de los requisitos esenciales de alto riesgo y simplemente se exigirán obligaciones específicas de trasparencia de los riesgos limitados o mínimos, como, por ejemplo, que los usuarios sean conscientes de que están interactuando con una máquina.

Y, en segundo lugar, porque en la mayor parte de los sistemas de IA considerados de alto riesgo en el trabajo, los efectos apreciables de impacto negativo en la seguridad de las personas son de carácter psicológico (por ej. el estrés y patologías psicosomáticas derivadas del monitoreo continuo de la actividad del trabajador o la conectividad constante en el trabajo en plataformas) y se van generando paulatinamente, de forma que, a priori podría no ser considerado de alto riesgo a la luz de la Ley de IA, porque, en realidad, como observan KULLMAN y CEFALIELLO, el impacto nocivo no aparece inmediatamente; es un proceso gradual"[25]

No obstante, aquellos proveedores que consideren que un sistema de IA no es de alto riesgo, pese a estar contemplado en el anexo III, deberán realizar y documentar una evaluación antes de que dicho sistema sea introducido en el mercado o puesto en servicio (art. 6.4 RIA). En esta evaluación se debe acreditar que el sistema de IA no plantea

[23] FERNÁNDEZ HERNÁNDEZ, C. Y EGUILUZ CASTAÑEIRA, J. A.: "Diez puntos críticos del Reglamento europeo de Inteligencia Artificial", *Diario La Ley*, nº 85, *Sección Ciberderecho*, 28 de junio de 2024.

[24] GOÑI SEIN, J. L.: "El Reglamento UE de Inteligencia Artificial y su interrelación con la normativa de seguridad y salud en el trabajo", AA. VV. (Dirs. EGUSQUIZA, M. A.; RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial…,* op. cit. pp. 103-4.

[25] KULLMAN, M. y CEFALIELLO, A.: "The interconnection between the AI Act and the EU's Occupational Safety and Health Legal Framework", January de 2022, disponible en http://global-workplace-law-and-policy.kluwerlawonline.com/2022/01/24/the-interconnection-between-the-ai-act-and-the-eus occupational-safety-and-health-legal-framework/

un riesgo significativo de daño a la salud, la seguridad o los derechos fundamentales de las personas físicas[26]. En todo caso, dichos proveedores estarán sujetos a la obligación de registro establecida en el artículo 49, apartado 2. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación (art. 6.4 RIA).

4. Implicaciones dañosas derivadas de la ia relacionadas con la seguridad y salud laboral

A la hora de valorar las implicaciones dañosas derivadas de los sistemas de IA, el intérprete debe tener en cuenta, asimismo, el distinto concepto de daño o perjuicio que lleva implícito la materialización del riesgo en cada una de las dos normativas de IA y de prevención de riesgos laborales.

En la normativa preventiva laboral, el concepto legal de daño derivado del riesgo laboral se concreta en "enfermedades, patologías o lesiones sufridas con motivo u ocasión del trabajo (art. 4.3 LPRL), englobando, también, los daños psicosociales que traen causa de la interacción del trabajador con la máquina.

Sin embargo, el concepto de daño en el RIA es más heterogéneo y plantea alguna otra dimensión añadida a la de seguridad y salud, relacionada con la posible vulneración de derechos fundamentales.

De entrada, toma en consideración los daños y perjuicios que sufran las personas o bienes como consecuencia del uso de los sistemas de IA. Los posibles perjuicios pueden ser resultado de defectos en el diseño general de los sistemas de IA, de un funcionamiento incorrecto, o de incidentes graves asociados al uso de sus sistemas de IA, y se concretan, bien en daños graves para la salud de las personas trabajadoras, o bien en una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas, o daños graves a la propiedad o al medio ambiente.

Dentro de esta amplia gama de daños, se deben considerar los impactos emocionales, como la ansiedad y el estrés, la pérdida de control, el asilamiento si interactúan solo con sistemas de IA o la pérdida de significado o de propósito, que son los riesgos más habitualmente notificados con relación a la utilización de los sistemas de IA en el lugar de trabajo. El uso intensivo de sistemas de gestión de personas basadas en la IA que obliga a los trabajadores a trabajar más rápido o que les mantiene estar continuamente conectados, o contantemente vigilados o controlados, puede provocar elevados niveles de estrés laboral, ansiedad y depresión con los consiguientes efectos sobre la salud[27].

Pero el perjuicio considerado por el RIA va más allá, relacionándose, además, con el incumplimiento de obligaciones derivadas del Derecho de la Unión destinadas a pro-

[26] FERNÁNDEZ HERNÁNDEZ, C. Y EGUILUZ CASTAÑEIRA, J. A.: "Diez puntos críticos del Reglamento europeo de Inteligencia Artificial", *Diario La Ley*, op cit.

[27] EU-OSHA: "Inteligencia Artificial para la gestión de las personas trabajadoras: riesgos y oportunidades". 10/08/2022, Disponible en: https://osha.europa.eu/es/publications/artificial-intelligence-worker-management-risks-and-opportunities.

teger los derechos fundamentales, señaladamente con el tratamiento de los datos digitales de las personas. El uso de los sistemas de IA puede deparar consecuencias perjudiciales de control invasivo, de discriminación o de uso ilícito de datos personales, de forma que ciertas personas pueden ver vulnerada su intimidad, o ser discriminadas en las valoraciones, ascensos, o extinciones, por hacer suposiciones en función de sus características.

En este sentido, incorpora una dimensión que podríamos calificar de "carácter moral"[28], puesto que se valoran también las consecuencias adversas de un sistema de IA para los derechos fundamentales de las personas de la Unión, protegidos por la Carta de Derechos de la UE. Se mencionan, entre otros, el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, y en especial la no discriminación (Considerando 48), que no interesan desde un punto de vista estrictamente preventivo de seguridad y salud laboral.

Puede suceder que determinados algoritmos de la IA capturen patrones ocultos que reflejen prejuicios humanos como el racismo, el sexismo, la discriminación por edad. Los sistemas de IA empleados, por ejemplo, para controlar el rendimiento y el comportamiento de las personas pueden acabar socavando los derechos fundamentales a la protección de datos personales y a la intimidad" (Considerando 57), causando un perjuicio moral por vulneración de derechos fundamentales y no físico, que dé lugar una indemnización de daños y perjuicios.

5. Obligaciones preventivas laborales del proveedor de sistemas de IA

Ya se ha comentado que el RIA ha tratado de conectarse con el Derecho de la Unión en materia relativa a las condiciones de empleo y de trabajo, incluidas la salud y seguridad en el trabajo (Considerando 9)[29], por lo que debe ser interpretado en consonancia con la normativa de prevención de riesgos laborales, en particular, Directiva 89/391 CEE, Marco de seguridad y salud laboral y la normativa interna de trasposición (LPRL).

A fin de proteger los derechos de los trabajadores frente a los riesgos de seguridad y salud derivados del uso de los sistemas de IA en el lugar de trabajo, los proveedores deben ser capaces de incorporar a sus diseños y desarrollos los aspectos de prevención de riesgos laborales como cuestión de interés público, al igual que otras medidas en lo que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas.

[28] RODRÍGUEZ SANZ DE GALDEANO, B.: "La responsabilidad empresarial por accidentes vinculados a la Inteligencia Artificial", *Trabajo y Derecho*, nº 19, junio 2024.

[29] Considerando 9: "*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 a la legislación laboral nacional —conforme al 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*".

No obstante, las obligaciones del proveedor de sistemas de IA varían según la clase de IA y el tipo de riesgo que comportan. El RIA establece, por un lado, distintas normas específicas para los modelos de IA de uso general sin riesgos sistémicos y para los modelos de IA con riesgos sistémicos, que deben aplicarse también cuando estos modelos estén integrados en un sistema de IA o formen parte de un sistema de IA; y, por otro lado, normas específicas para los sistemas de IA.

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

Es preciso diferenciar el concepto de modelos de IA de uso general del concepto de sistemas de IA con el fin de garantizar la seguridad jurídica. Los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen por sí mismos sistemas de IA. Los modelos de IA requieren que se les añadan otros componentes, como, por ejemplo, una interfaz de usuario, para convertirse en sistemas de IA. Los modelos de IA suelen estar integrados en los sistemas de IA y formar parte de dichos sistemas (Considerando 97).

Por otra parte, dentro de los modelos de IA de uso general debe diferenciarse entre los modelos de IA sin riesgo sistémico y modelos de IA con riesgo sistémico, que conllevan, 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" (Considerando 110).

Los modelos de IA de uso general sin riesgo sistémico deben cumplir una serie de obligaciones y requisitos establecidos en el artículo 53 RIA. Son fundamentalmente medidas de transparencia proporcionadas, lo que incluye elaborar documentación y mantenerla actualizada y facilitar información sobre el modelo de IA de uso general, incluida la información relativa al proceso de entrenamiento y realización de pruebas y los resultados de su evaluación, para su uso por parte de los proveedores posteriores.

El proveedor del modelo de IA de uso general tiene la obligación de 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. Esta información debe permitir a los proveedores de sistemas de IA entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones. Los elementos mínimos que debe contener dicha documentación se encuentran en los anexos XI y XII específicos del Reglamento.

Un modelo de IA de uso general presenta riesgos sistémicos cuando tiene capacidades de gran impacto —evaluadas mediante herramientas y metodologías técnicas adecuadas— o unas repercusiones considerables en el mercado interior debido a su alcance. 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. Cuando se alcanza un umbral inicial de ope-

raciones de coma flotante se presume que el modelo es un modelo de IA de uso general con riesgos sistémicos (Considerando 111).

La Comisión puede 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, atendiendo a una evaluación global de los criterios para la designación de modelos de IA de uso general con riesgo sistémico establecidos en un anexo del presente Reglamento, como la calidad o el tamaño del conjunto de datos de entrenamiento, el número de usuarios profesionales y finales, sus modalidades de entrada y de salida, su nivel de autonomía y escalabilidad o las herramientas a las que tiene acceso. Y ello particularmente cuando 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 (Considerando 113)

Los modelos de IA de uso general con riesgo sistémico están sujetos, además de a las obligaciones impuestas a los proveedores de modelos de IA de uso general, a las específicas establecidas en el artículo 55 del Reglamento. Estas incluyen 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

Además, los proveedores de estos modelos de IA deben realizar una evaluación de riesgos y mitigar continuamente los riesgos sistémicos, por ejemplo, mediante el establecimiento de políticas de gestión de riesgos, como procesos de rendición de cuentas y gobernanza, la puesta en práctica de la vigilancia poscomercialización, la adopción de medidas adecuadas durante todo el ciclo de vida del modelo y la cooperación con los agentes pertinentes a lo largo de la cadena de valor de la IA. Si, a pesar de los esfuerzos por detectar y prevenir los riesgos, 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 (Considerando 115).

Por lo que respecta a las obligaciones preventivas de seguridad y salud laboral, hay que tener en cuenta que cuando los modelos de IA se integran en sistemas de IA se deben seguir aplicando, además de las obligaciones establecidas en el Reglamento IA en relación con los modelos de IA, las establecidas en relación con los sistemas de IA. Por tanto respecto de las obligaciones en materia preventiva hay que estar a lo que a continuación se indicará sobre las obligaciones preventivas del proveedor de los sistemas de IA de alto riesgo.

5.2. Obligaciones de proveedores de sistemas de IA de alto riesgo

Con carácter general, los proveedores que comercialicen o pongan en servicio sistemas de IA de alto riesgo en la Unión, con independencia de que dichos proveedores estén

establecidos o ubicados en la Unión o un tercer país, se encuentran obligados a observar una serie de requisitos previstos en el art. 16 del capítulo III.

Entre ellos, el primero y básico es que los sistemas de IA de alto riesgo cumplan los requisitos establecidos sección 2 del capítulo III , "*teniendo en cuenta sus finalidades previstas y el estado actual de la técnica generalmente reconocido en materia de IA*" (art. 8 RIA). Los requisitos de los sistemas de IA de alto riesgo establecidos en la sección 2 del capítulo III, se resumen básicamente en los siguientes: establecimiento, documentación y mantenimiento de un sistema de gestión de riesgos (art. 9) (incluida la evaluación previa de conformidad); aseguramiento de la alta calidad de datos utilizados en el entrenamiento del sistema para minimizar riesgos y resultados discriminatorios (art. 10); disponer de una precisa documentación que cumpla con los requisitos del Anexo IV (art. 11); garantizar la trazabilidad del funcionamiento del sistema mediante un registro de actividad (art. 12); ofrecer una información clara y adecuada al responsable del despliegue para que lo interprete y use correctamente (art. 13)[30]; contar con medidas de vigilancia humana, dotándolos de herramientas de interfaz humano-máquina para prevenir o reducir al mínimo los riesgos que pueden surgir del uso adecuado a la finalidad

[30] Art. 13 RIA*: "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, y en particular:

i) su finalidad prevista;

ii) el nivel de precisión (incluidos los parámetros para evaluarla), 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 su información de salida;

v) cuando proceda, su funcionamiento con respecto a personas o grupos de personas específicos 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;

vii) en su caso, información que permita a los responsables del despliegue interpretar la información 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 vigilancia humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA 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 permitir a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro de conformidad con el artículo 12".

como del uso indebido razonablemente previsible (art. 14); ofrecer un nivel adecuado de precisión, solidez, y ciberseguridad durante todo su ciclo de vida, adoptando las medidas técnica y organizativas necesarias (art. 15).

A ello se unen las obligaciones de: colocar en el embalaje del sistema de IA su nombre comercial y dirección de contacto; disponer de un sistema de gestión de calidad (art. 17); conservar la documentación relativa a técnica, sistema de gestión de la calidad, cambios aprobados, declaración UE de conformidad (art. 18); conservar los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 19; asegurar que los sistemas de IA de alto riesgo sean sometidos al procedimiento pertinente de evaluación de la conformidad antes de su introducción en el mercado o puesta en servicio (ex art 43); elaborar una declaración UE de conformidad (ex art. 47); colocar en el sistema de IA de alto riesgo, en su embalaje o documentación el marcado CE de conformidad con el presente Reglamento (ex art. 48); cumplir las obligaciones de registro (ex art. 49.1); establecer medidas correctoras cuando tenga motivos para ello, retirando desactivando o recuperando; velar por que el sistema de IA de alto riesgo cumpla requisitos de accesibilidad productos y servicios.

Lo señalado solo es de aplicación, como ya se ha indicado antes, a los proveedores que despliegan un sistema de IA que merezca la consideración de alto riesgo por entrañar un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por el RIA. En consecuencia, de no influir sustancialmente en la toma de decisiones ni perjudicar dichos intereses sustancialmente", no resulta de aplicación. Así lo remarca, por otra parte, el art. 6.3 RIA: "N*o obstante lo dispuesto en el apartado 2, un sistema de IA no se considerará de alto riesgo si no plantea un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, en particular al no influir sustancialmente en el resultado de la toma de decisiones.*

En particular, el artículo 6.3 RIA considera que los sistemas de IA no entrañan dicho riesgo importante, y, en consecuencia, no constituyen alto riesgo cuando *se cumplan una o varias de las condiciones siguientes:*

a) que el sistema de IA tenga por objeto llevar a cabo una tarea de procedimiento limitada;
b) que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada;
c) que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; o
d) que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III".

De todas formas, es esencial indicar que un sistema de IA será considerado de alto riesgo si realiza una elaboración de perfiles o perfilado de personas física, dejando

inoperativas las excepciones anteriormente mencionadas[31]. Dispone, en este sentido, el art. 6.3 RIA, en su último párrafo, que: "*No obstante lo dispuesto en el párrafo primero, los sistemas de IA a que se refiere el anexo III siempre se considerarán de alto riesgo cuando el sistema de IA lleve a cabo la elaboración de perfiles de personas físicas*". Este elemento introduce "una dinámica potencialmente conflictiva donde los sistemas de IA, de otro modo evaluados como de bajo riesgo, pueden categorizarse en un estatus de alto riesgo únicamente debido a las características integradas, independientemente de su impacto real de riesgo real"[32].

Nos encontramos, así, con una sucesión encadenada de reglas técnicas, bastante abstractas, de excepción y contra excepción, que atenúan y debilitan la percepción de los principios y garantías que deben cumplir los sistemas de IA de alto riesgo. Su inespecificidad hace complicado y confuso anticipar cuándo se está ante un sistema de IA sujeto a las obligaciones aplicables con carácter general a los sistemas de IA de alto riesgo.

No obstante, de lo expuesto se deriva que puede haber sistemas de IA de alto riesgo que, aun catalogados como tales, no lo son porque no entrañan riesgos importantes, y otros que no siendo de alto riesgo por no causar daño considerable, pueden ser, sin embargo, catalogados como tales, porque así lo ha determinado el RIA, que serían los casos en los que se lleve a cabo la elaboración de perfiles de personas físicas.

En todo caso, el proveedor siempre podrá disipar las posibles dudas de aplicación de la serie de obligaciones que contempla la sección 2 del Capítulo III, acogiéndose a alguno de los mecanismos de acreditación de conformidad de los sistemas de IA de alto riesgo, y con ello podrá conjurar cualquier eventual responsabilidad por no haber adoptado dichas medidas.

El proveedor puede optar por aplicar las normas armonizadas publicadas en el DOUE a que se refiere el artículo 40, o bien, en su caso, las especificaciones comunes emitidas por organismos a que se refiere el artículo 41, o el procedimiento de evaluación de la conformidad, basado en el procedimiento interno de control, establecido en el anexo VI, o los certificados emitidos por los organismos competentes (ex art. 44) que serán válidos para el período que indiquen, que no excederá de cuatro años para los sistemas de IA contemplados en el anexo III[33].

Por tanto, una posibilidad, entre otras, sería diseñar los sistemas de IA siguiendo las normas armonizadas del art. 40 , y someterse a los correspondientes procedimientos de evaluación de conformidad (art. 43). El art. 40 establece que "*se presumirá que los sistemas de IA de alto riesgo que sean conformes con normas armonizadas, o partes de estas, cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea de conformidad con el Reglamento (UE) n.º 1025/2012 son conformes con los requisitos establecidos en la*

[31] FERNÁNDEZ HERNÁNDEZ, C. Y EGUILUZ CASTAÑEIRA, J. A.: "Diez puntos críticos del Reglamento europeo de Inteligencia Artificial", *Diario La Ley,* op cit.

[32] Ibidem.

[33] A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales no superiores a cuatro años para los sistemas de IA contemplados en el anexo III, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables.

sección 2 del presente capítulo o, en su caso, con las obligaciones establecidas en el capítulo IV del presente Reglamento, en la medida en que dichas normas abarquen estos requisitos u obligaciones". El problema radica en que no se cuenta todavía con esas normas técnicas actualizadas que recojan los estándares técnicos de seguridad[34].

Adentrándonos en el terreno específico de las obligaciones preventivas laborales del proveedor, es preciso distinguir entre los sistemas de IA sujetos a los requisitos de alto riesgo y los que no están obligados a ello.

1) En los sistemas de IA de alto riesgo, destinados a ser utilizados en el trabajo, que cumplan los requisitos establecidos sección 2 del capítulo III y entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por el RIA, y en aquellos otros sistemas de IA que, sin comportar un riesgo importante, "*se consideran de alto riesgo por llevar a cabo la elaboración de perfiles de personas físicas"*, la previsión de riesgos laborales constituye una parte esencial de la declaración de conformidad, porque según lo previsto en el art. 8 RIA, deben tener en cuenta "*sus finalidades previstas y el estado actual de la técnica generalmente reconocido en materia de IA*".

Tanto si se trata de sistema de IA de alto riesgo destinado a ser utilizado como componente de una máquina, como si se considera un producto en sí mismo, siempre que sean diseñados para ser utilizados en el trabajo, el proveedor está obligado a garantizar que el sistema de IA de alto riesgo ha sido entrenado, validado y probado con datos que reflejen el entorno geográfico, conductual contextual o funcional específico en el que esté previsto su uso (art. 42 RIA).

Dichas prácticas habrán de realizarse teniendo en cuenta, según el art. 10 RIA, el diseño, los procesos de recogida de datos, la finalidad original de la recogida, las operaciones de tratamiento de datos, la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos; 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; y las medidas adecuadas para detectar, prevenir y reducir posibles sesgos detectados.

Es decir, el proveedor deberá tener muy presente la finalidad del sistema de IA y los datos que se van a recabar, deberá entrenar con datos que reflejen el entorno en que se va a utilizar el sistema de IA, y prever los posibles riesgos para la seguridad y salud laboral y la violación de los derechos fundamentales, así como estimar la magnitud de los mismos, y tomar una decisión apropiada sobre las medidas que deben adoptarse de prevención de riesgos laborales.

[34] RODRÍGUEZ SANZ DE GALDEANO, B.: "La responsabilidad empresarial por accidentes vinculados a la Inteligencia Artificial", *Trabajo y Derecho*, nº 19, junio 2024.

El RIA ha tratado de conectar los requisitos del Reglamento IA con otras normas sectoriales de la Unión, indicando, como ya se ha reiterado, que "*completan el conjunto existente de actos de armonización de la Unión*". En este sentido, los sistemas de IA destinados a ser integrados en máquinas, habrán de ajustarse a las especificaciones que indica la normativa de máquinas, en concreto, el Reglamento (UE) 2023/1230, relativo a máquinas y por el que se deroga la Directiva 2006/42/CE y la Directiva 73/361/CEE, (no aplicable hasta el 20 de enero de 2027), que ha venido precisamente a regular los nuevos riesgos emergentes de la Inteligencia artificial y el Internet de las cosas (IoT). De igual modo, en el supuesto de sistemas de IA destinados a ser incorporados a equipos de protección individual, será necesario que cumplan con su normativa específica; en este caso, el Reglamento 2016/425 que prevé los requisitos esenciales de seguridad que han de reunir estos equipos. Y todo ello sin perjuicio del deber de ajustarse a la normativa de protección de datos, aspecto no abordado en este estudio [35]

A esta premisa acompaña luego, como ulterior corolario, el deber de todo fabricante de productos o equipos de cumplir, de acuerdo con lo dispuesto en el art. 41 LPRL, las obligaciones generales de seguridad. Aquí pueden surgir algunas fricciones, porque la primera obligación del fabricante es que la maquinaria, los equipos, productos y útiles de trabajo "no constituyan una fuente de peligro" (art. 41.1 LPRL), y el RIA no garantiza, sin embargo, el mismo nivel de protección por cuanto no excluye un riesgo alto si no causa un perjuicio considerable, como hemos señalado. Ocurre, además, que los valores del RIA no son solo de seguridad sino también de mercado; y por tanto la comercialización se ha convertido en rasgo esencial. Con lo cual, la aplicación íntegra de las obligaciones del art. 41 LPRL al proveedor de sistemas de IA resulta insostenible y obliga a una afinación o reformulación de las mismas, reconociendo su relatividad respecto al modo de concretarse en el trabajo.

2) En el caso de los sistemas de IA que no representan un alto riesgo (riesgo medio o bajo), los requisitos de seguridad previstos en el RIA se traducen generalmente en obligaciones de transparencia o información que permitan a los usuarios ser conscientes de que interactúan con un sistema de IA y comprender sus características y limitaciones. Así se establece, por ejemplo, como ya se apuntado anteriormente, con respecto a los sistemas de IA diseñados para interactuar con personas (chatbots); o en el caso de los sistemas de IA, incluidos los sistemas de uso general, debiendo garantizar que los resultados del sistema

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

> de IA estén marcados en un formato legible por máquina y detectable como generado o manipulado artificialmente; o con relación a los sistemas de reconocimiento de emociones y sistemas de clasificación biométrica, obligando a informar de que se están usando; o en los sistemas que generen o manipulen imágenes o audio de personas (ultrafalsificación) teniendo que informar de que se trata de imágenes o sonidos manipulados artificialmente.

Es poco probable el empleo de estos sistemas de IA en el trabajo, pero, de ser utilizados en el trabajo, en principio, les resultaría de aplicación las obligaciones preventivas laborales previstas genéricamente en el art. 41 de la LPRL para el fabricante de productos de trabajo. Como en el caso anterior, el proveedor de tales sistemas vendría obligado a: asegurar que éstos no constituyen una fuente de peligro para el trabajador; a envasar y etiquetar correctamente de forma que se permita su conservación y manipulación en condiciones de seguridad, e identificar claramente los riesgos para la seguridad y salud de los trabajadores que su utilización comporten; y a proporcionar información sobre la forma correcta de utilización las medidas preventivas adicionales y los riesgos laborales que conlleva tanto su uso normal como su manipulación o empleo inadecuado[36].

Ahora bien, en tales casos volverían a chocar los fines preventivos laborales con los del RIA que aspira también a facilitar la libre circulación y el reconocimiento de los sistemas de IA y a promover el comercio internacional de la industria de la IA. No está, por tanto, muy claro que los proveedores de estos sistemas de IA de riesgo medio o bajo estén obligados a cumplir estrictamente cada una de las exigencias del art. 41 LPRL, dado que ello daría lugar, además, al establecimiento de unas garantías de exigencia de seguridad más altas, que en los de riesgo alto, lo que carece de toda lógica.

6. Obligaciones preventivas del empresario respecto de los sistemas de IA

El Reglamento de IA prevé también obligaciones para los responsables de la implantación de los sistemas de IA de alto riesgo, esto es, para los empresarios en cuanto usuarios o implementadores de tales productos que tengan su lugar de establecimiento, o estén situados, en la Unión (art. 2.1 RIA). Ellos conocen mejor que nadie el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, *"detectar potenciales riesgos significativos que no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los grupos de personas que probablemente se vean afectados, entre los que se incluyen grupos de personas vulnerables*" (Considerando 93).

Las obligaciones impuestas al empresario por el art. 26 del RIA tienen un carácter marcadamente instrumental en la medida que aspiran a garantizar fundamentalmente la correcta aplicación del sistema de IA de alto riesgo, conforme a las indicaciones de uso dadas por el proveedor o fabricante del mismo. Dentro del amplio elenco de obli-

[36] FRANCIS LEFEBVRE: *Memento Social. Prevención de Riesgos Laborales*, *2024-2025*, Madrid , p. 1416.

gaciones, es posible distinguir entre: A) las obligaciones previas a la puesta en servicio o utilización del sistema de IA del alto riesgo (obligaciones de diseño), y B) las relativas al despliegue o uso del mismo (obligaciones de uso).

A) Obligaciones de diseño. Antes de poner en servicio, el empresario se encuentra obligado a: 1) adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas de conformidad con sus instrucciones de uso; 2) encomendar la supervisión humana a personas físicas con competencia y formación necesarias; 3) asegurarse de que los datos de entrada sean pertinentes y suficientemente representativos para la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos, 4) e informar 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 (art. 26. 1, 2, 4 y 7 RIA). Pero para ello el empresario debe estar correctamente informado de las características, las capacidades y las limitaciones del funcionamiento del sistema de IA.

A tal fin, el Reglamento exige al fabricante transparencia respecto de los sistemas de IA de alto riesgo, de modo que permita al empresario comprender la manera en que el sistema de IA funciona, evaluar su funcionalidad y comprender sus fortalezas y limitaciones. Estos elementos abarcarían, según precisa el Considerando 72, *la información sobre las posibles circunstancias conocidas o previsibles relacionadas con el uso del sistema de IA de alto riesgo, incluida la actuación del responsable del despliegue capaz de influir en el comportamiento y el funcionamiento del sistema, en cuyo marco el sistema de IA puede dar lugar a riesgos para la salud, la seguridad y los derechos fundamentales, sobre los cambios que el proveedor haya predeterminado y evaluado para comprobar su conformidad y sobre las medidas pertinentes de supervisión humana, incluidas las medidas para facilitar la interpretación de la información de salida del sistema de IA por parte de los responsables del despliegue. La transparencia, incluidas las instrucciones de uso que acompañan a los sistemas de IA, debe ayudar a los responsables del despliegue a utilizar el sistema y tomar decisiones con conocimiento de causa*.

Del conjunto de obligaciones señaladas, se desprende que el empresario asume en relación con la adopción de la IA de alto riesgo los siguientes compromisos (de los que cabe colegir eventualmente responsabilidades): el primero, estar informado sobre los usos previstos y excluidos; el segundo, elegir correctamente el sistema de IA de alto riesgo en función de los usos previstos y no excluidos (la adopción de estos sistemas de IA debe responder a un fin permitido)[37]; el tercero, garantizar que el personal que se encargue de la supervisión tiene el nivel de formación necesario (la alfabetización en materia de inteligencia artificial y los conocimientos necesarios para garantizar el cumplimiento adecuado

[37] Considerando 74 RIA : *El nivel previsto de los parámetros de funcionamiento debe declararse en las instrucciones de uso que acompañen a los sistemas de IA*.

y la correcta ejecución la debe proporcionar el empresario)[38]; y el cuarto, informar tanto a la representación legal de los trabajadores como a los trabajadores afectados de los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución.

Sobre estas obligaciones se interfieren las derivadas de la normativa de protección de datos (RGPD y LOPDGDD), que, entre otras exigencias, impone realizar una evaluación de impacto sobre los derechos fundamentales de los sistemas de IA de alto riesgo (art. 27 RIA) (asunto que merece un tratamiento específico), pero cuyos resultados bien pudieran limitar la adopción de los sistemas de IA si esta tecnología entra en conflicto con dicha normativa[39]. El cumplimiento de las obligaciones del RIA aplicables a los sistemas de IA debe entenderse sin perjuicio de otras obligaciones a los responsables del despliegue de sistemas de IA establecidas en el Derecho de la Unión o nacional, como las señaladas de protección de datos personales.

B) Obligaciones de uso. Una vez implantado el sistema de IA de alto riesgo, el empleador debe ejercer un control sobre los datos de entrada, garantizar que dichos datos sean pertinentes y suficientemente representativos a la vista de la finalidad prevista del sistema, supervisar el funcionamiento del sistema sobre la base de las instrucciones de uso , informar al proveedor cuando el sistema presente un riesgo, suspendiendo el uso del sistema, y conservar los registros generados automáticamente por el sistema durante un periodo adecuado a la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses (art. 26. 3,4, 5 y 6 RIA)

A ello se añade la obligación del empleador que usa el sistema de IA de alto riesgo de los incluidos en el Anexo III, de informar a las personas físicas (trabajadores) de que están expuestas a la utilización de los sistemas de la IA de alto riesgo (art. 26.7 RIA). Y si, además, se ven afectadas por una decisión que el responsable adopte basándose en los resultados de un sistema de IA de alto riesgo y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de forma que considere que tiene un efecto perjudicial para la salud, su seguridad o sus derechos fundamentales, tendrán derecho a obtener del empresario explicaciones claras y significativas acerca del papel que el sistema ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

Anótese además, que los responsables del despliegue que utilicen un sistema de IA para generar o manipular un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeje notablemente a personas, lugares o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos (ultrafalsificaciones) están

[38] Considerando 91 RIA: *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*.

[39] RODRÍGUEZ SANZ DE GALDEANO, B.: La responsabilidad empresarial por accidentes vinculados a la Inteligencia Artificial", Trabajo y Derecho, op. cit.

obligadas también a hacer público, de manera clara y distinguible, que este contenido ha sido creado o manipulado, de manera artificial etiquetando la información de salida generada por la inteligencia artificial en consecuencia e indicando su origen artificial. En tales casos, el deber de transparencia en relación con las ultrafalsificaciones obliga al empresario a revelar la existencia de tales contenidos generados o manipulados (Considerando 134).

El deber empresarial de garantizar, conforme al RIA, la seguridad y salud en los sistemas de IA de alto riesgo es correlativo al deber de protección de los proveedores. Por tanto, sus obligaciones específicas como responsable de la implantación son exigibles únicamente respecto de aquellos sistemas de IA que cumplan los requisitos establecidos en la sección 2 del capítulo III y entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por el RIA y aquellos otros sistemas de IA que, sin comportar un riesgo importante, se consideran de alto riesgo por llevar a cabo la elaboración de perfiles de personas físicas.

No obstante, el alcance de sus obligaciones preventivas no se agota en la dimensión prevista por el RIA, sino que se integra al mismo tiempo por el conjunto de obligaciones propias de prevención de riesgos laborales, que el empresario, como garante de la seguridad y salud laboral de las personas trabajadoras, debe asumir, conforme a la LPRL. Ni las obligaciones de los proveedores ni las obligaciones propias suyas derivadas del RIA, eximen al empresario de cumplir con las obligaciones específicas en materia de prevención de riesgos laborales.

Desde esta otra perspectiva preventiva laboral, y de acuerdo con la LPRL, el empresario debe garantizar la seguridad y salud de los trabajadores a su servicio, adoptando cuantas medidas sean necesarias y desarrollando una acción permanente de seguimiento de la actividad preventiva. En concreto, el empresario habrá de identificar, evaluar y controlar los riesgos que no se hayan podido evitar, adoptar las medidas preventivas adecuadas en el lugar de trabajo, así como informar a los trabajadores sobre los riesgos que no se hayan podido evitar y formarles para el adecuado manejo de los equipos[40].

Y todo ello con respecto de cualquier dispositivo de IA y. no solo con relación a los sistemas de IA de alto riesgo que, según el RIA, entrañan un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por el RIA y aquellos otros sistemas de IA que, sin comportar un riesgo importante, se consideran de alto riesgo por llevar a cabo la elaboración de perfiles de personas física, dado el deber del empresario de adoptar cuantas medidas sean necesarias para evitar el daño cualquiera que sea.

7. Conclusiones

El Reglamento de IA tiene en común con la LPRL el elemento esencial del riesgo, pues ha sido diseñado bajo el enfoque del riesgo que la puesta en marcha y uso de determina-

[40] RODRÍGUEZ SANZ DE GALDEANO, B.: La responsabilidad empresarial por accidentes vinculados a la Inteligencia Artificial", Trabajo y Derecho, op. cit.

dos sistemas de IA plantean para la salud, la seguridad y derechos fundamentales consagrados en la Carta. Ambos comparten también el objeto porque, mientras la LPRL trata de identificar y estimar la magnitud del riesgo para posteriormente evitarlo o, en su caso, reducirlo y controlarlo[41], el RIA impone a los proveedores obligaciones orientadas a evaluar riesgos concretos y a aplicar medidas de reducción del riesgo razonable; su control constituye, por tanto, el objetivo clave de la actividad preventiva.

Pero hay elementos que separan a ambas normativas. Ante todo, la propia caracterización del riesgo. La LPRL acoge un criterio general, sin exclusiones o distinciones de categorías de riesgo; el deber de prevención laboral se extiende a cualquier tipo de riesgo. Sin embargo, el RIA limita sus exigencias a determinados tipos y categorías de riesgos. La Propuesta inicial de Reglamento de IA solo contemplaba la gama de "riesgos crónicos" (inaceptable, alto, limitado y mínimo), pero, a consecuencia de la aparición de los denominados GPAI, (los General Purpose AI sistems and models) se ha insertado una nueva regulación de los modelos y sistemas de IA de uso general, que puede plantear riesgos sistémicos. Por tanto, el RIA distingue entre dos grandes categorías: los riesgos sistémicos, de muy reducida probabilidad pero de una intensidad e implicaciones mucho más graves; y los riesgos crónicos de alta frecuencia pero de intensidad moderada.

Por otra parte, el riesgo tomado en consideración por el RIA se contrae a los sistemas de IA que presentan un "riesgo considerable" 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". Junto a ello el RIA considera que la calificación de alto riesgo debe formularse previendo reducir al mínimo cualquier restricción del comercio internacional, pues tiene como objetivo promover el desarrollo responsable y sostenible de la IA en la Unión Europea, mediante la creación de un marco normativo armonizado y proporcional para la IA, que reduzca la fragmentación del mercado interno.

Todos estos condicionantes de magnitud del riesgo o de orden económico establecidos por el RIA sobre los sistemas de IA de alto riesgo hacen presagiar una limitada aplicación del RIA en el ámbito de las relaciones laborales por cuanto buena parte de los sistemas de IA utilizados en el ámbito laboral (la mayoría son de gestión de recursos humanos) no presentan de entrada un efecto nocivo grave o alto a los trabajadores, y porque el impacto negativo, muchas veces de carácter psicológico, no aparece de forma súbita sino de forma gradual. Ahora bien, no cabe obviar que los sistemas de IA, a pesar de no enmarcarse en el Anexo III también pueden categorizarse en un estatus de alto riesgo independientemente de su riesgo real, si realizan una elaboración de perfiles ex art. 6.3 RIA, por lo que es muy probable que muchos de los sistemas de IA utilizados actualmente en gestión de recursos humanos acaben siendo considerados sistemas de alto riesgo por esta vía de excepción.

[41] Así, entre los principios generales del deber general de prevención laboral (art. 15.1 LPRL), se hallan los de evitar los riesgos, evaluar los riesgos que no se puedan evitar, y combatir los riesgos en su origen

De todas formas, y con independencia de ello, el proveedor, que asume la mayor parte de las obligaciones preventivas que establece el RIA, debe tener en cuenta en el diseño y desarrollo de los sistemas de IA los aspectos de prevención de riesgos laborales como cuestión de interés público, porque el alcance de sus obligaciones preventivas no se agota en la dimensión prevista por el RIA, sino que se integra al mismo tiempo por el conjunto de obligaciones propias de prevención de riesgos laborales, que el fabricante, como garante de la seguridad y salud laboral de las personas trabajadoras, debe asumir, conforme al art. 41 de la LPRL.

Por otra parte, el empleador/usuario de los sistemas de IA en el lugar de trabajo debe tener presente que ni las obligaciones de los proveedores, ni las obligaciones propias suyas derivadas del RIA, le eximen de cumplir con las obligaciones específicas en materia de prevención de riesgos laborales que le impone la LPRL. Su deber empresarial de protección de la seguridad y salud laboral de las personas trabajadoras se superpone a las obligaciones del RIA, proyectándose, además, no solo sobre los sistemas de IA de alto riesgo que, según el RIA, entrañan un riesgo considerable de causar un perjuicio importante, sino también sobre cualquier dispositivo de IA con independencia de la categoría de riesgo que comporte.

8. Bibliografía consultada

ABDULLAH MALIK: *Artificial Intelligence in Health and Safety*, 22 /2/ 2023. Disponible en: https://safetypedia-com.translate.goog/safety/artificial-intelligence-in-health-and safety/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc

BARRIO ANDRÉS, M. : "Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial", *Diario LA LEY, Nº 86, Sección Ciberderecho*, 30 de Julio de 2024.

FERNÁNDEZ HERNÁNDEZ, C. y EGUILUZ CASTAÑEIRA, J. A.: "Diez puntos críticos del Reglamento europeo de Inteligencia Artificial", *Diario LA LEY, Nº 85, Sección Ciberderecho*, 28 de junio de 2024.

FRANCIS LEFEBVRE: *Memento Social. Prevención de Riesgos Laborales*, 2024-2025, Madrid , 2024, p. 1416.

GOÑI SEIN, J. L.: "El Reglamento UE de Inteligencia Artificial y su interrelación con la normativa de seguridad y salud en el trabajo", AA. VV. (Dirs. EGUSQUIZA, M. A.; RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades*, Tirant lo Blanch, Valencia 2023,

GOÑI SEIN,J.L.; RODRÍGUEZ SANZ DE GALDEANO, B.; LLORENS ESPADA, J.; MARIN MALO, M.: "El impacto del nuevo marco normativo europeo de la inteligencia artificial en las relaciones laborales", AA VV (Dir. RICHARD GONZÁLEZ, M.), en prensa edit J B. Bosch.

KULLMAN, M. y CEFALIELLO, A.: "The interconnection between the AI Act and the EU's Occupational Safety and Health Legal Framework", January de

2022, Disponible en http://global-workplace-law-and-policy.kluwerlawonline.com/2022/01/24/the-interconnection-between-the-ai-act-and-the-eusoccupational-safety-and-health-legal-framework/

LLORENS ESPADA, J.: *Límites al uso de la Inteligencia Artificial en el ámbito de la salud*, La Ley, Madrid, 2023, pp. 151 y ss.

LLORENS ESPADA, J.: "Inteligencia artificial y salud laboral", AA. VV. (Dirs. EGUSQUIZA, M. A.; RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades*, Tirant lo Blanch, Valencia 2023.

MERCADER UGUINA, J.: "Los usos de alto riesgo en el ámbito laboral de la IA y la certificación", *El Foro de Labos,* 9/5/2024, Disponible en: https://www.elforodelabos.es/2024/05/los-usos-de-alto-riesgo-en-el-ambito-laboral-de-la-ia-y-la-autocertificacion/

RODRÍGUEZ SANZ DE GALDEANO, B.: "La responsabilidad empresarial por accidentes vinculados a la Inteligencia Artificial", *Trabajo y Derecho,* nº 19, junio 2024.

VESTRI, G.: "La Unión Europea estrena el Reglamento de Inteligencia Artificial (RIA). Control, supervisión y uso de una tecnología cada vez más presente en la vida de todos", *Diario LA LEY*, Nº 10550, 19 de Julio de 2024.