ISSN: 1696-3083, Revista Galega de Dereito Social -2ª ET- (18,2023), pp. 41-74
http://www.revistagalegadedereitosocial.gal

OBLIGACIONES DEL EMPRESARIO EN MATERIA DE PREVENCIÓN DE RIESGOS LABORALES DERIVADAS DE LA UTILIZACIÓN DE SISTEMAS DE IA*

BEATRIZ RODRÍGUEZ SANZ DE GALDEANO
Profesora Titular de Derecho del Trabajo y de la Seguridad Social
Universidad Pública de Navarra
beatriz.rodriguez@unavarra.es

RESUMEN

El objetivo de del presente estudio es analizar cuáles son las obligaciones del empresario que incorpora productos de trabajo o sistemas de software basados en la Inteligencia Artificial. Para ello, se realiza una caracterización genérica de estos nuevos desarrollos tecnológicos y de las oportunidades y retos que plantean en materia preventiva. Posteriormente, se desciende al análisis de cuáles son las obligaciones del empresario que incorpora estos nuevos equipos con fines productivos, de gestión de recursos humanos o para el cumplimiento de sus obligaciones preventivas. Para ello, se parte, en primer lugar, de la normativa general de seguridad de los productos y de la normativa específica sobre sistemas de IA; en segundo lugar, se analizan las obligaciones derivadas de la normativa de protección de datos cuando se introducen equipos dotados con sistemas de IA que implican un tratamiento de datos; por último, se estudian las obligaciones específicas en materia de prevención de riesgos laborales, ahondando en sus conexiones con la nueva normativa sobre IA.

* Artículo realizado en el marco las actividades de investigación correspondientes al Proyecto de Generación del Conocimiento "Inteligencia Artificial y Prevención de Riesgos Laborales: retos para la normativa preventiva y en materia de responsabilidad" (PID2021-123514NB-I00), IP: Prof. Dr. José Luis Goñi Sein. Universidad Pública de Navarra.

Recibido: 02/06/2023; Aceptado: 20/07/2023

Palabras clave: Inteligencia Artificial; Seguridad del Producto; Obligaciones Preventivas del Empresario; Responsabilidad civil por productos defectuosos.

RESUMO
O obxectivo do presente estudo é analizar cales son as obrigas do empresario que incorpora produtos de traballo ou sistemas de *software* baseados na intelixencia artificial. Para iso, realízase unha caracterización xenérica destes novos desenvolvementos tecnolóxicos e das oportunidades e retos que formulan en materia preventiva. Posteriormente, descéndese á análise de cales son as obrigas do empresario que incorpora estes novos equipos con fins produtivos, de xestión de recursos humanos ou para o cumprimento das súas obrigas preventivas. Para iso, pártese, en primeiro lugar, da normativa xeral de seguridade dos produtos e da normativa específica sobre sistemas de IA; en segundo lugar, analízanse as obrigas derivadas da normativa de protección de datos cando se introducen equipos dotados con sistemas de IA que implican un tratamento de datos; por último, estúdanse as obrigas específicas en materia de prevención de riscos laborais, profundando nas súas conexións coa nova normativa sobre IA.
Palabras chave: Intelixencia artificial; seguridade do produto; obrigas preventivas do empresario; responsabilidade civil por produtos defectuosos.

SUMARIO

CAUCES DE COORDINACIÓN EN MATERIA DE EVALUACIÓN ENTRE LA PROPUESTA DE LEY DE IA Y LA NORMATIVA SECTORIAL DE SEGURIDAD DEL PRODUCTO. **3. LAS OBLIGACIONES DEL EMPRESARIO EN CUANTO USUARIO DE PRODUCTOS BASADOS EN SISTEMA DE IA DERIVADAS DE LA NORMATIVA EN MATERIA DE SEGURIDAD DEL PRODUCTO Y DE LA LEY IA;** 3.1. UTILIZACIÓN CONFORME AL USO PREVISTO O RAZONABLEMENTE PREVISIBLE; 3.2. OBLIGACIONES ESPECÍFICAS PARA EL USUARIO DE SISTEMAS DE IA; 3.3.- EL EMPRESARIO COMO FABRICANTE: LA ALTERACIÓN DEL PRODUCTO O SISTEMA DE IA. **4. LAS OBLIGACIONES DEL EMPRESARIO EN MATERIA PREVENTIVA. 5. LAS OBLIGACIONES DEL EMPRESARIO EN MATERIA DE PROTECCIÓN DE DATOS. 6. APROXIMACIÓN A LA NUEVA NORMATIVA EN MATERIA DE RESPONSABILIDAD CIVIL DERIVADA DE PRODUCTOS DEFECTUOSOS Y POR DAÑOS CAUSADOS POR SISTEMAS DE IA. 7. BIBLIOGRAFÍA.**

1. INTRODUCCIÓN: INCORPORACIÓN DE LA IA EN LA EMPRESA Y SU IMPACTO EN MATERIA DE PREVENCIÓN DE RIESGOS LABORALES

Los desarrollos tecnológicos basados en sistemas de Inteligencia Artificial (en adelante IA), están siendo incorporados a la organización productiva de la empresa de diversos modos y con diferentes finalidades.

Es ya una realidad la utilización de equipos robóticos avanzados que incorporan sistemas de IA, con el fin de mejorar su eficacia y asegurar su adecuado mantenimiento y supervisión[1]. La incorporación a los robots tradicionales de sensores capaces de interactuar con el entorno y de sistemas de tratamiento de datos para ejecutar tareas de forma autónoma, ha dado lugar a una nueva generación de robots, que está liderando en gran medida la nueva revolución industrial. Estos equipos pueden ser adquiridos por el

[1]EU-OSHA: *Advanced robotics and automation: implications for occupationl safety and health,* 2022, disponible en: https://osha.europa.eu/en/publications/advanced-robotics-and-automation-implications-occupational-safety-and-health

empresario directamente del fabricante, se trataría, por tanto, de productos que incorporan ya soluciones basadas en sistemas de IA. Pero también es posible que el empresario adquiera directamente sistemas de IA con el fin de incorporarlos a sus propios equipos para mejorar o desarrollar ciertas utilidades. En estos casos, el fin primordial del empresario suele ser incorporarlos a su organización productiva para mejorar el rendimiento.

Asimismo, los equipos que incorporan sistemas de IA, también pueden adquirirse por el empresario con el fin de destinarlos al cumplimiento de determinadas obligaciones preventivas. Es el caso, por ejemplo, de los drones basados en sistemas de IA, que se utilizan con el fin de supervisar las condiciones de seguridad en las que se desarrollan determinadas operaciones complejas. Con ello, el empresario puede cumplir las obligaciones específicas de coordinación y supervisión, que le impone la normativa preventiva.

También comienza a ser frecuente la utilización de software, basado en IA, con fines de gestión de recursos humanos [2]. Se trata de programas informáticos que permiten obtener información sobre el desarrollo del trabajo, rendimiento de los equipos, etc., con el fin genéricamente de mejorar la productividad y eficiencia de la empresa. En ocasiones este software se incorpora a los propios equipos de trabajo con el fin de tener un conocimiento óptimo y en tiempo real sobre el funcionamiento de estos equipos. Estos sistemas se basan en el procesamiento de datos, personales o no.

Estos sistemas entrañan en la mayoría de las ocasiones un control del propio trabajador y, desde este punto de vista, puede que las decisiones que se adopten puedan consistir en la simple formulación de recomendaciones sobre la forma correcta de desarrollar el trabajo, o que pretendan la evaluación del trabajador y de sus posibles errores o incluso servir como base para la adopción de medidas disciplinarias[3].

---

[2] EU-OSHA: *Artificial intelligence for worker management: an overview,* 2022, disponible en https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-overview

[3] EU-OSHA: *Artificial intelligence for worker management: mapping definitions, uses and implications,* 2022, disponible en:

Este *sofware*, puede ser adquirido directamente por el empresario y, en tal caso, como se verá, habrá de asegurarse de que responde a los requerimientos de seguridad y observar el resto de normativa preventiva y en materia de protección de datos. Aunque también puede ocurrir que el empresario no adquiera directamente este software, sino que opte por contratar a un tercero, que utiliza este tipo de sistemas con el fin de prestar un servicio relativo, por ejemplo, al control de incapacidades, del estado de salud de los trabajadores, etc.

Desde el punto de vista legislativo estos avances tecnológicos requieren adaptaciones de un marco normativo que, en su actual configuración, no ofrece respuesta a los principales interrogantes que plantea esta nueva revolución. Como en anteriores ocasiones, la evolución de la técnica se sitúa un paso por delante del marco normativo vigente. Junto a ello, la revolución tecnológica actual, a diferencia de otras anteriores, se caracteriza por su complejidad y por su rápida extensión a las más diversas áreas vitales.

Por otro lado, ha de tenerse en cuenta que cualquier intervención legislativa ha de ponderar los diversos intereses en juego. No cabe duda de que resulta necesario asegurar un nivel adecuado de seguridad y prevención de los riesgos que estos nuevos avances entrañan, sin desconocer al mismo tiempo el impacto positivo que pueden tener en nuestro desarrollo vital y los importantes intereses económicos en juego.

A la luz de este panorama brevemente descrito, la cuestión que se plantea, dejando al lado los supuestos de contratación de servicios con terceros, es cuáles son las obligaciones que ha de asumir el empresario que incorpora este tipo de productos basados en sistemas de IA a su empresa.

Para abordar esta cuestión es necesario conjugar tres bloques normativos diversos: por un lado, la normativa de seguridad del producto, incluida la propuesta de Reglamento de IA, por otro lado, la normativa en materia de prevención de riesgos laborales y, por último, la normativa en materia

https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-mapping-definitions-uses-and-implications

de protección de datos. No se aborda con detenimiento las posibles responsabilidades por los daños causados por tales productos, si bien, se dedica un breve apartado final a la presentación de los avances normativos que en el ámbito de la responsabilidad civil se están impulsando desde Europa.

2. LA OBLIGACIÓN DE ADQUIRIR PRODUCTOS SEGUROS Y EL IMPACTO DE LA PROPUESTA DE LEY DE IA

La primera obligación del empresario que incorpora productos basados en sistemas de IA es asegurarse de que dichos productos cumplan con la normativa existente en materia de seguridad del producto. Para ello, el fabricante habrá de tener en cuenta, en primer lugar, las disposiciones específicas, si existen, relativas al concreto producto (máquinas, EPIs, etc.) y, en segundo lugar, los requisitos de seguridad para sistemas basados en IA exigidos por la nueva Ley de IA.

2.1. NORMATIVA ESPECÍFICA DE SEGURIDAD DEL PRODUCTO: EL NUEVO ENFOQUE EN MATERIA DE ARMONIZACIÓN TÉCNICA

La normativa de seguridad del producto tiene como objetivo principal garantizar un nivel elevado de seguridad de los productos que se comercializan en la UE y evitar los obstáculos al libre comercio. Para conseguir este objetivo la normativa de seguridad se basa en el denominado nuevo enfoque en materia de armonización, con el que se pretende garantizar una adaptación rápida de las exigencias de seguridad[4]. Para ello, las directivas o reglamentos comunitarios se limitan a recoger los requisitos de seguridad que deben reunir los productos. El fabricante que pretenda comercializar un producto en la UE ha de llevar a cabo las evaluaciones del producto con el fin de acreditar que reúne los requisitos de seguridad. Para facilitar este proceso se presume la conformidad a los requisitos esenciales de seguridad de aquellos productos que cumplan las normas

[4] Resolución del Consejo de 17 de mayo de 1985, relativa a una nueva aproximación en materia de armonización y de normalización.

técnicas, de carácter voluntario, elaboradas por los organismos de normalización. De tal manera, que la observación de estas normas técnicas facilite el proceso de evaluación de la conformidad. Los productos que cumplan los requisitos de seguridad pueden incorporar el marcado CE y la declaración CE de conformidad.

En lo que se refiere específicamente a los equipos tradicionalmente destinados a un uso profesional, existe una normativa consolidada basada en el nuevo enfoque para productos tales como: máquinas, equipos de protección individual, equipos a presión, etc.

Este sistema tradicional, ha permitido una armonización rápida de las exigencias esenciales de seguridad, gracias a la efectividad de los organismos de normalización, que han realizado una importante labor de actualización de las normas técnicas, sin perder de vista el objetivo de garantizar un elevado nivel de seguridad. Sin embargo, el desarrollo de productos basados en sistemas de IA obliga a la UE a revisar su actuación en materia de seguridad del producto. Con este objetivo desde la UE, ha venido trabajando en la propuesta de Reglamento IA, que a continuación se detalla.

2.2. NORMATIVA DE SEGURIDAD RELATIVA A LOS SISTEMAS DE IA: APROXIMACIÓN BASADA EN EL RIESGO

A la hora de abordar la regulación de los requisitos de seguridad de los sistemas de IA la UE se marcó un doble objetivo, por un lado, dotar de un marco normativo suficiente para garantizar un nivel adecuado de seguridad de los sistemas de IA que se comercializan en Europa, por otro lado, coordinar estas nuevas exigencias con la ya consolidada normativa existente en materia de seguridad del producto.

Con este doble objetivo, la UE ha apostado por una norma horizontal, la propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial)[5], la propuesta inicial ha sido objeto de multitud de enmiendas, que fueron

[5] COM (20221) 106 final, de 21 de abril de 2021.

aprobadas por el Parlamento Europeo el pasado 14 de junio de 2023[6].

La última propuesta, tras las enmiendas adoptadas, incorpora, en su art. 4 bis, los principios que han de guiar la actuación de todos los operadores y que son los siguientes: intervención y vigilancia humana, solidez y seguridad técnica, privacidad y gobernanza de datos, transparencia, respeto a la diversidad y no discriminación y bienestar social y medioambiental.

La nueva norma opta por definir en términos amplios su ámbito de aplicación y ofrecer un marco general, basado en la clasificación de riesgos. El art. 3.1 define sistema de IA como: *"un sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía y capaz, para objetivos explícitos o implícitos, de generar información de salida —como predicciones, recomendaciones o decisiones— que influya en entornos reales o virtuales".*

Una vez definido en términos tan amplios el concepto de sistema de IA, la norma opta por un enfoque basado en el riesgo, para concretar los requisitos de seguridad exigidos para la puesta en circulación de estos servicios, en función de si se está ante sistemas prohibidos, sistemas de alto riesgo y el resto de sistemas[7].

Por otro lado, con el objeto de facilitar la coordinación con la normativa ya existente en materia de seguridad, el texto del Reglamento recoge los requisitos esenciales de seguridad que han de reunir determinados sistemas de IA, considerados de alto riesgo, pero ha previsto que los productos que ya eran objeto de normativa específica se sigan rigiendo por dicha normativa, aunque también han de respetar los requisitos esenciales de seguridad en materia de IA.

En lo que se refiere a la convivencia de esta normativa con la específica en materia laboral, el Reglamento en su art. 2 apartado 5 quater, señala que la aplicación de lo dispuesto

[6] La última versión, con las enmiendas aprobadas, se puede consultar en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.pdf

[7] Goñi Sein, J.L. (2023): Ley de inteligencia artificial y seguridad y salud en el trabajo", en AA.VV. (dir.: Rodríguez Sanz de Galdeano, B. y Egusquiza Balmaseda, M.A.: *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.

en el Reglamento, no impide que los Estados introduzcan normas más favorables para los trabajadores o permitan la aplicación de convenios colectivos más favorables.

2.2.1. Sistemas prohibidos

La propuesta de Ley de IA prohíbe en su art. 5 una serie de sistemas entre los que se incluyen: aquéllos basados en el uso de las técnicas subliminales, manipuladoras o engañosas que puedan alterar el comportamiento humano; sistemas de IA para la explotación de puntos débiles de grupos de personas que sean vulnerables por su edad, capacidad, situación social o económica, cuando se causa con tales prácticas un perjuicio significativo; sistemas de categorización biométrica que clasifiquen a la persona con arreglo a atributos o características sensibles o protegidas; sistemas que sirvan para la calificación social de personas físicas en razón de sus características, personalidad, que conduzcan a un trato injustificado o desproporcionado de personas o grupos, o a un trato perjudicial; sistemas de identificación biométrica remota en tiempo real en espacios de acceso público; sistemas de IA para llevar a cabo evaluaciones de riesgo de personas con el fin de determinar el riesgo de que cometan infracciones y los sistemas que creen o amplíen bases de datos de reconocimiento facial mediante extracción de imágenes faciales a partir de internet o circuito cerrado de televisión; sistemas para inferir emociones entre otros ámbitos, en el lugar de trabajo y sistemas de identificación biométrica en diferido, salvo que estén sujetos a una autorización judicial y sean necesarios para la búsqueda selectiva destinada a la aplicación de la ley y relacionada con un delito grave.

Se trata, como puede observarse, de sistemas que contravienen los valores de la Unión de respeto a la dignidad humana, libertad, igualdad, democracia y Estado de Derecho y de los derechos fundamentales, que reconoce la UE, como el derecho a la no discriminación, la protección de datos y la privacidad.

2.2.2. Sistemas de alto riesgo

Entre los sistemas de alto riesgo se incluyen, en primer lugar, aquellos destinados a ser utilizados como componente de seguridad de uno de los productos contemplados en el Anexo II de la propuesta y también aquellos sistemas que en sí mismos son uno de estos productos, siempre que estos productos conforme a su propia legislación de armonización deban someterse a una evaluación externa. Entre los productos que recoge el Anexo se encuentran, productos sometidos a la normativa del nuevo enfoque y destinados a ser utilizados en el ámbito profesional tales como las máquinas, equipos de protección individual, equipos a presión, aparatos para uso en atmósferas explosivas, ascensores. Ahora bien, no basta con que el sistema de IA se incorpore o sea uno de estos productos, sino que además es necesario que requiera evaluación de conformidad de un tercero. Este tipo de evaluaciones de conformidad se contemplan en la normativa sectorial de seguridad de cada producto y su imposición depende del grado de peligrosidad. Así, por ejemplo, en el caso de las máquinas se requiere dicha evaluación por tercero cuando se trate de alguna de las máquinas incluidas en el Anexo IV entre las que figuran sierras, plataformas elevadoras, máquinas moldeadoras, máquinas portátiles de impacto, etc.

En segundo lugar, se consideran sistemas de alto riesgo, según el art. 6.2 de la propuesta, los mencionados en el Anexo III con la condición, añadida tras el trámite de enmiendas, de que entrañen un riesgo significativo de causar perjuicios para la salud, la seguridad o los derechos fundamentales de las personas físicas. El Anexo toma como criterio el uso y el ámbito al que se destina el sistema de IA. En lo que aquí interesa, se incluyen sistemas destinados a ser utilizados para extraer conclusiones sobre las características físicas de las personas a partir de datos biométricos; sistemas dirigidos a evaluar el nivel de educación de una persona e influir en el nivel de educación y formación que va a recibir; sistemas para la contratación y la selección de trabajadores y los sistemas destinados a adoptar decisiones en materia de promoción o asignación de tareas, evaluación del rendimiento

y conducta de los trabajadores en el marco de dichas relaciones; sistemas de IA destinados a ser utilizados en sus sistemas de recomendación por plataformas de redes sociales, designadas como plataformas en línea de muy gran tamaño. Ha de tenerse en cuenta que, tras el trámite de enmiendas, se ha introducido en el art. 6 un apartado 2 bis, en virtud del cual se permite a los proveedores presentar una notificación motivada a la autoridad nacional de supervisión cuando consideren que su sistema de IA no presenta un riesgo significativo.

La propuesta de Ley de IA obliga al fabricante de estos sistemas de alto riesgo a implantar, documentar y mantener un sistema de gestión de riesgos que incluye: la identificación, la estimación y la evaluación de los riesgos conocidos y razonablemente previsibles para la seguridad y la salud, para los derechos fundamentales, incluida la igualdad de acceso y de oportunidades, la democracia o el medio ambiente, cuando se utilice conforme a la finalidad prevista o en condiciones de uso indebido razonablemente previsibles; la evaluación de los riesgos significativos emergentes; la adopción de las medidas oportunas de gestión de riesgos. (art. 9). Además, en el caso de que los sistemas de IA utilicen técnicas que implican el entrenamiento con modelos de datos, habrán de cumplirse los criterios de calidad previstos en los apartados 2 a 5 del art. 10 de la propuesta, entre los que se incluye un examen que atienda a la existencia de sesgos que puedan dar lugar a discriminaciones prohibidas.

El proceso se completa con la previsión de un sistema de evaluación de la conformidad (art. 43), dirigido a demostrar el cumplimiento de los requisitos de seguridad exigidos por el Reglamento. Cuando se supere dicha evaluación de conformidad, los sistemas de IA incorporarán el marcado CE de conformidad. Se añade, además, que los sistemas de IA de alto riesgo que sean conformes con normas armonizadas se entenderán conformes con los requisitos esenciales de seguridad. Se observa como el esquema trazado para garantizar la seguridad de estos sistemas de alto riesgo se basa en la filosofía inspiradora del nuevo enfoque en materia de armonización. Ocurre, sin embargo, que en la actualidad

no existe una referencia de especificaciones técnicas en materia de IA, similar a la existente para otros productos como máquinas o EPIs. Por ello, como novedad, la propuesta de IA contempla la posibilidad de que la Comisión elabore especificaciones comunes, que recojan estándares técnicos. Estas especificaciones se aprobarán para el caso de que no haya normas armonizadas o cuando sean insuficientes. Para su elaboración la Comisión ha de recabar los puntos de vista de los organismos y grupos de expertos pertinentes.

2.2.3. Sistemas que no son de alto riesgo

Los proveedores de sistemas que no sean considerados de alto riesgo según la propuesta de ley de IA, podrán voluntariamente cumplir los requisitos de seguridad impuestos a los sistemas de alto riesgo. Con el objeto de promover esta aplicación voluntaria, se establece que la Comisión y el Comité promoverán la elaboración de códigos de conducta tendentes a facilitar el cumplimiento de los requisitos de seguridad (art. 69).

Se abre, por tanto, un espacio no regulado, que en buena medida dependerá del desarrollo de esos códigos de conducta y de su utilidad para el desarrollo de sistemas de IA que no son de alto riesgo.

2.2.4. Obligaciones de transparencia para determinados sistemas de IA

El art. 52 de la propuesta contempla obligaciones para los sistemas de IA, sean o no de alto riesgo, destinados a interactuar con personas físicas. En estos casos se deberá informar por el sistema de IA o por el propio proveedor o usuario a las personas expuestas de que están interactuando con un sistema de IA, salvo cuando resulte evidente. Además, se informará cuando proceda, de las funciones habilitadas por la IA, de si existe vigilancia humana y de quién es el responsable de la toma de decisiones.

2.3. CAUCES DE COORDINACIÓN EN MATERIA DE EVALUACIÓN ENTRE LA PROPUESTA DE LEY DE IA Y LA NORMATIVA SECTORIAL DE SEGURIDAD DEL PRODUCTO

Tal y como se ha visto, los sistemas de IA pueden integrarse en equipos ya existentes, por ejemplo, una máquina o un EPI, con el fin de mejorar su eficacia o introducir nuevas utilidades. En estos casos, se plantea la necesidad de coordinar las exigencias de seguridad específicas, contempladas en la normativa sectorial de cada producto y las exigencias de seguridad propias de los sistemas de IA de alto riesgo.

Para ello, la propuesta de ley de IA ha previsto que en tales casos los equipos se sometan a la evaluación de conformidad, de acuerdo con la normativa sectorial específica, y que, en el marco de dicho proceso de evaluación de la conformidad, se compruebe también el cumplimiento de los requisitos obligatorios relativos a los sistemas de IA de alto riesgo. De tal manera que el marcado CE, acreditará el cumplimiento de los requisitos de seguridad del concreto producto y también del sistema de IA.

3. LAS OBLIGACIONES DEL EMPRESARIO EN CUANTO USUARIO DE PRODUCTOS BASADOS EN SISTEMAS DE IA DERIVADAS DE LA NORMATIVA EN MATERIA DE SEGURIDAD DEL PRODUCTO Y DE LA LEY IA

La normativa que establece los requisitos de seguridad de los productos tiene como principal destinatario al proveedor de tales productos. Tal y como se ha visto, el fabricante será quien deba observar los requisitos obligatorios de seguridad y acreditar su cumplimiento mediante la correspondiente evaluación de conformidad. De tal manera que la principal obligación del empresario será asegurarse de que los productos que adquiere son seguros.

Ahora bien, más allá de este momento inicial de adquisición del producto, durante su utilización el empresario, en cuanto usuario del mismo, ha de observar una serie de obligaciones que derivan directamente de la normativa de seguridad del producto y que, en el caso de utilización de sistemas de IA, presentan especialidades derivadas de las particularidades de este tipo de sistemas, motivadas fundamentalmente porque

su comportamiento se puede ver alterado con posterioridad a la comercialización.

3.1. UTILIZACIÓN CONFORME AL USO PREVISTO O RAZONABLEMENTE PREVISIBLE

Con carácter general, el empresario está obligado a utilizar los equipos para los fines para los que fueron diseñados, así lo contempla expresamente el art. 41 LPRL. Desde un punto de vista concreto, en la definición de seguridad contenida en la Directiva sobre Seguridad general de los productos y en la propuesta de Reglamento general, el concepto de producto seguro se relaciona con los usos razonables del mismo[8]. De tal manera, que el fabricante ha de garantizar un nivel elevado de seguridad en tales condiciones. En contrapartida, el empresario ha de utilizar los productos para los fines para los que fueron diseñados y que razonablemente cabe esperar. En la normativa específica sectorial, se reiteran estas referencias al uso previsto en condiciones razonables.

En lo que se refiere en particular a los sistemas de IA, el art. 3 de la propuesta de ley IA, tras las enmiendas del Parlamento, ha preferido optar por la denominación de implementador, en lugar de usuario, para referirse a la persona como física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. De acuerdo con esta definición, el empresario que utiliza el sistema de IA como medio de producción en su empresa, tendría la condición de implementador a efectos de la IA. Este rol del empresario, añade nuevas obligaciones a las tradicionalmente recogidas por la normativa de seguridad del producto y prevención de riesgos laborales.

Las obligaciones que la propuesta impone a los implementadores se refieren a los casos de utilización de sistemas calificados como de alto riesgo. Estos sistemas, tal

[8] Directiva 2001/95, de 3 de diciembre. Está siendo objeto de revisión y en la actualidad existe ya una Propuesta, de 30 de junio de 2021, del Parlamento Europeo y del Consejo, relativa a la seguridad general de los productos, COM 2021/346 final.

y como se ha visto anteriormente, son aquellos sistemas de IA que son un producto sometido a legislación de armonización o un componente de seguridad de dichos productos y que, conforme a su normativa específica, la evaluación de conformidad precisa la intervención de un organismo independiente. Asimismo, han de considerarse de alto riesgo lo sistemas de IA utilizados en el ámbito del empleo para alguna de las finalidades recogidas en el apartado 4 del Anexo III.

Con carácter general y ahondando en la obligación de utilizar los productos conforme a su finalidad, la propuesta de ley de IA, introduce una serie de obligaciones que incumben fundamentalmente al proveedor, con el fin de asegurar que el usuario, el empresario en este caso, realiza un uso adecuado de los sistemas. Así, el art. 9.4 c) incluye entre las medidas de gestión de riesgos, la información sobre los riesgos derivados de un uso adecuado y de un uso indebido razonablemente previsible. A estos efectos, se señala que se tendrá en cuenta la experiencia, educación y formación del usuario y que, cuando proceda, puede resultar necesario impartir formación a los usuarios. El art. 13 se refiere específicamente al modo en que ha de trasladarse la información a los usuarios y señala que se ha de garantizar que los sistemas funcionen con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente la información de salida. Además, señala que deberán ir acompañados de las instrucciones de uso adecuadas, que deben incluir información concisa, completa, correcta y clara, de manera pertinente, accesible y comprensible. En concreto, señala que esta información debe especificar la finalidad prevista, cualquier circunstancia asociada a su utilización prevista o uso indebido razonable que pueda dar lugar a un riesgo, su funcionamiento en relación con personas que puedan utilizar tales sistemas, la vida útil del sistema, las medidas de vigilancia humana que deben adoptarse y las medidas de mantenimiento y cuidado, incluyendo lo referido a la actualización del software.

3.2. OBLIGACIONES ESPECÍFICAS PARA EL IMPLEMENTADOR DE SISTEMAS DE IA

Al margen de estas obligaciones destinadas fundamentalmente a garantizar un uso adecuado del sistema de IA, conforme a su diseño, la propuesta de ley de IA, introduce obligaciones nuevas, derivadas de las peculiaridades propias de los sistemas de IA, que no han tenido precedente en la normativa sectorial específica de seguridad del producto.

Así, el art. 14 obliga a arbitrar medidas de vigilancia humana respecto de los sistemas de alto riesgo durante su tiempo de funcionamiento. El objetivo de esta vigilancia es reducir al mínimo posibles riesgos para la salud, seguridad o derechos fundamentales. En el caso de utilización de estos sistemas en el ámbito laboral, será el empresario el encargado de garantizar estas medidas de vigilancia humana de acuerdo con la información que le haya facilitado el proveedor y que debe especificarse en la documentación técnica.

Asimismo, el empresario como usuario de un sistema de alto riesgo, ha de observar las obligaciones recogidas en el art. 29 de la propuesta de Ley de IA, entre las que se incluyen: asegurarse de que los datos de entrada son pertinentes para la finalidad prevista del sistema de IA; aplicar las medidas de supervisión humana necesarias, vigilar el funcionamiento del sistema e informar de posibles incidentes; interrumpir si fuera necesario su funcionamiento e informar a las autoridades en caso necesario; conservar los archivos de registro que se generan automáticamente y utilizar la información facilitada para cumplir la obligación de evaluación de impacto relativa a la protección de datos. Además, los usuarios de sistemas de IA de alto riesgo deberán conservar los archivos de registro que tales sistemas generen, en la medida en que estén bajo su control.

Por otro lado, el art. 61 de la propuesta de ley de IA introduce obligaciones de seguimiento posterior a la comercialización que incumben fundamentalmente a los proveedores, pero que también pueden implicar a los usuarios. En general, se obliga a los proveedores a establecer y documentar un sistema de seguimiento posterior a la comercialización y se señala que dicho sistema recabará datos pertinentes sobre el

funcionamiento de los sistemas de IA. Estos datos pueden ser proporcionados por los usuarios, en nuestro caso el empresario, o mediante otras fuentes.

Por último, el art. 52 de la propuesta de ley de IA, obliga a los usuarios de sistemas de IA que generen o manipulen contenido de imagen, sonido o vídeo que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puedan inducir a considerar que son reales, a hacer público que el contenido ha sido generado de forma artificial. Esta situación podría generarse cuando se utilicen simulaciones en el ámbito preventivo, con fines de información, formación o adiestramiento. Este mismo artículo, según se ha visto, obliga también a los usuarios de sistemas de IA destinados a interactuar con personas físicas a informar a las personas expuestas de que están interactuando con sistemas de IA.

3.3. EL EMPRESARIO COMO FABRICANTE: LA ALTERACIÓN DEL PRODUCTO O SISTEMA DE IA

Con carácter general las obligaciones sobre los requisitos de seguridad de los productos tienen como destinatario principal al fabricante, proveedor o importador que comercializa el producto en la UE. Sin embargo, puede haber ocasiones en las que el producto, una vez comercializado, sufra alteraciones. En este caso la normativa de seguridad del producto, cuando dichas alteraciones sean sustanciales, considera que se está ante un nuevo producto y que la persona que ha introducido tales alteraciones ha de ser considerada fabricante y, en consecuencia, ha de someter nuevamente el producto al cumplimiento de los requisitos esenciales de seguridad.

Así la Guía azul sobre aplicación de las normas de producto, señala que: "Un producto que ha sido objeto de cambios o de revisiones para modificar sus prestaciones, sus fines o su tipo originales puede ser considerado un producto nuevo. La persona que lleva a cabo los cambios se convertirá en el fabricante y deberá asumir las obligaciones correspondientes. Las actualizaciones de software o las reparaciones pueden ser incluidas entre las operaciones de mantenimiento siempre que no modifiquen un producto ya introducido en el mercado

de tal manera que puedan afectar a su observancia de los requisitos vigentes."[9]

En la misma línea la propuesta de Reglamento relativo a la seguridad general de los productos[10], en su art. 12.1 señala que: "Se considerará fabricante a efectos del presente Reglamento a las personas físicas o jurídicas, distintas del fabricante, que modifiquen sustancialmente el producto; y estarán sujetas a las obligaciones que impone al fabricante el artículo 8 en lo que respecta a la parte del producto afectada por la modificación o a la totalidad del producto si la modificación sustancial repercute en su seguridad. 2. Se considerará que una modificación es sustancial cuando se cumplan los tres criterios siguientes:

a) la modificación altera las funciones, el tipo o el rendimiento previstos del producto de una manera que no estaba contemplada en la evaluación inicial del riesgo del producto;

b) la naturaleza del peligro ha cambiado o el nivel de riesgo ha aumentado debido a la modificación;

c) los cambios no han sido realizados por el consumidor para su propio uso."

En lo que se refiere a la normativa específica, directamente relativa a equipos de trabajo, ha de destacarse que también la propuesta de Reglamento de máquinas, tiene como objetivo expreso aclarar el concepto de modificación sustancial, que ya se recogía en la Directiva actualmente vigente[11]. Así, el art. 15 de la propuesta, titulado: "otros casos en que son aplicables las obligaciones de los fabricantes" señala expresamente que: "A los efectos del presente Reglamento, se considerará fabricante a una persona física o jurídica, distinta del fabricante, el importador o el distribuidor, que lleve a cabo una modificación sustancial de la máquina, la parte o el accesorio, y que, por consiguiente, estará sujeta a las obligaciones del fabricante establecidas en el artículo 10 con respecto a la pieza del producto afectada por la modificación o, si la modificación

[9] Guía azul sobre la aplicación de las normas de producto de la UE, 2014, pág. 18.

[10] COM (2021) 346 final, de 30 de junio de 2021.

[11] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativa a las máquinas y sus partes y accesorios COM (2021) 202, final.

sustancial afecta a la seguridad del producto en su conjunto, con respecto a todo el producto".

Por su parte, el art. 3, en su apartado 16 define modificación sustancial como: "una modificación de una máquina, una parte o un accesorio, por medios físicos o digitales, después de que dicho producto se haya introducido en el mercado o puesto en servicio, que no haya sido prevista por el fabricante y debido a la cual pueda verse afectada la conformidad del producto con los requisitos esenciales de salud y seguridad".

En el caso de los sistemas de IA, también la propuesta de ley de IA ha contemplado expresamente esta posibilidad y ha incluido una definición de qué debe entenderse modificación sustancial, en su art. 3.23, que la define como: "una modificación o serie de modificaciones en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido prevista o proyectada por el proveedor en la evaluación de riesgos inicial y a consecuencia de la cual resulte afectado el cumplimiento por parte del sistema de IA dos requisitos establecidos en el título III, capítulo 2, del presente Reglamento o se modifique la finalidad prevista para la que se ha evaluado al sistema de IA en cuestión."

De acuerdo con lo anterior, el empresario puede erigirse en fabricante y, por tanto, estar obligado a verificar la conformidad del producto cuando introduzca cambios sustanciales en el equipo. La cuestión trascendental es cómo concretar el significado de modificación sustancial y diferenciarlo de otras modificaciones que no entrañan tal carácter sustancial y que pueden considerarse meras actualizaciones. Parece que el elemento determinante se encuentra en que la alteración no haya sido prevista por el fabricante y pueda afectar a los requisitos esenciales de seguridad. En coherencia con lo anterior, parece que las actualizaciones del equipo previstas por el fabricante no han de considerarse modificación sustancial porque, en principio, ya han sido tenidas en consideración en la evaluación inicial. Por ello, cuando el empresario se limite por ejemplo a actualizar el software conforme a las indicaciones del propio fabricante, no estaríamos ante un supuesto de modificación sustancial. Distinto sería el caso cuando el empresario actualiza una máquina, modificando su funcionamiento, sin

el acuerdo del fabricante o para un uso no previsto. Es en estos casos cuando el empresario se equipararía al fabricante y tendría, por tanto, que garantizar y acreditar el cumplimiento de los requisitos de seguridad y estampar un nuevo marcado CE.

4. LAS OBLIGACIONES DEL EMPRESARIO EN MATERIA PREVENTIVA

La normativa de seguridad del producto, aunque tiene como fin garantizar unos estándares elevados de seguridad, no siempre tiene en cuenta las peculiaridades derivadas de la utilización en un ámbito profesional de los equipos. La integración en el medio laboral de los productos entraña riesgos específicos que pueden tener su origen en el propio entorno laboral y en sus condicionantes físicos y medioambientales, en la organización del trabajo (ritmos de producción, reparto de tareas) o en las propias características de los trabajadores. La normativa de seguridad y salud en el trabajo erige al empresario en el principal obligado frente al trabajador, al que reconoce el derecho a una protección eficaz. Con el fin de ayudar al empresario en el cumplimiento de tan exigente obligación, la LPRL va desgranando una serie de obligaciones concretas, algunas de la cuales son desarrolladas en normativa específica. En lo que se refiere a los riesgos derivados de la utilización de equipos de trabajo, ha de estarse a lo dispuesto en el art. 41 LPRL, que obliga al empresario a utilizar los equipos conforme a los fines recomendados por el fabricante, a instalarlos y mantenerlos de forma adecuada y a informar y formar a los trabajadores sobre su utilización y posibles riesgos. De forma específica esta obligación general se desarrolla en el RD 1215/1992, de 18 de julio, sobre utilización por los trabajadores de los equipos de trabajo, el RD 486/97, de 14 de abril, sobre lugares de trabajo o el RD 485/1997, de 14 de abril, sobre señalización de seguridad y salud en el trabajo.

Asimismo, el empresario ha de realizar la oportuna evaluación de riesgos laborales, de acuerdo con lo dispuesto en el art. 16 LPRL y en los art. 3 y siguientes del RD 39/1997, de 17 de enero, que aprueba el Reglamento de los Servicios de Prevención. En esta evaluación han de tomarse en

consideración todos los riesgos derivados de la elección de equipos de trabajo. La evaluación, además, ha de mantenerse actualizada y revisarse cuando se hayan detectado daños o se aprecie que las actividades de prevención son insuficientes. Esta evaluación de riesgos ha de realizarse respecto de todos los equipos y productos utilizados en el trabajo y que puedan entrañar algún riesgo, lo cual significa, que la integración de sistemas de IA en la empresa, sean o no de alto riesgo, requiere la previa evaluación de riesgos.

La exigencia con que la normativa de prevención de riesgos laborales configura la obligación de seguridad del empresario y el amplio elenco de obligaciones específicas determina que, en la práctica, el empresario se convierta en el principal obligado frente al trabajador y ello a pesar de que también la normativa de prevención de riesgos impone al fabricante ciertas obligaciones. Junto a ello, existen también motivos de orden procesal, tales como la facilidad para entablar demanda frente al empresario y la inversión de la carga de la prueba, que explican que el empresario sea el principal objetivo de las reclamaciones por daños derivados de accidente.

Sin embargo, la complejidad de estos nuevos avances tecnológicos y la posibilidad de que existan riesgos desconocidos de cuyo alcance se tenga conocimiento después de la comercialización, aconsejarían una revisión de la separación entre las obligaciones empresariales y del fabricante.

Por otro lado, ha de tenerse en cuenta que el enfoque del Reglamento de IA, basado en un sistema de pirámide de riesgos, solo impone el cumplimiento de requisitos de seguridad a los sistemas de IA que sean considerados de alto riesgo. Además, tal y como se ha visto, la consideración como sistema de IA de alto riesgo, exige estar incluido en alguno de los usos especificados por el Anexo y que, además, el sistema entrañe un riesgo significativo. Esta opción del legislador, puede dar lugar a que existan sistemas que no son de alto riesgo, que se utilicen en el ámbito del trabajo y que, sin embargo, puedan entrañar riesgos para la seguridad y la salud o puedan, incluso, atentar a derechos fundamentales.

En otro orden de consideraciones, se apuntaba al inicio que el empresario puede recurrir a estos sistemas de IA con fines productivos, pero también para cumplir parte de sus obligaciones preventivas. Sería el caso, por ejemplo, de utilización de drones con sistemas de IA para coordinar determinadas actividades peligrosas, para apoyar la labor de los recursos preventivos o coordinadores de seguridad. Igualmente, puede ocurrir que el empresario requiera a software basado en IA para realizar determinadas verificaciones sobre el estado de salud de los trabajadores. No cabe duda de que la IA puede apoyar al empresario en el cumplimiento de este tipo de obligaciones. No obstante, a la hora de valorar su viabilidad ha de realizarse un análisis detenido de la LPRL y de su normativa de desarrollo. Así, por ejemplo, en lo referido a la coordinación de actividades o a la presencia del recurso preventivo, la LPRL es deudora de un modelo basado en la presencia física de la persona que, por lo tanto, no podrá ser sustituido por la utilización de otras soluciones tecnológicas, a pesar de su indudable utilidad. En lo que se refiere a la vigilancia de la salud, habrá de estarse a las posibilidades que para la realización de reconocimientos recoge el art. 22 LPRL y a las limitaciones propias del tratamiento de datos, que han de categorizarse como sensibles.

5. LAS OBLIGACIONES DEL EMPRESARIO EN MATERIA DE PROTECCIÓN DE DATOS

Una de las novedades principales de la incorporación de estos nuevos desarrollos tecnológicos con diferentes fines en la empresa es que en muchos casos traen consigo el tratamiento de datos del trabajador. Esta circunstancia hace necesario revisar el marco genérico de obligaciones que para el empresario se derivan del Reglamento (UE) 2016/679, de Parlamento Europeo y del Consejo, en materia de protección de datos (en adelante RGPD) y sus conexiones con la propuesta de ley de IA.

La propia propuesta de ley de IA en su justificación señala que debe aplicarse sin perjuicio del RGPD y en los considerandos señala que, a la hora de valorar la peligrosidad de un sistema de IA, ha de tenerse en cuenta sus

consecuencias adversas para derechos fundamentales como el de la protección de datos.

Estas declaraciones contrastan con la escasez de preceptos en la ley de IA referidos expresamente a las implicaciones en materia de protección de datos de los sistemas de IA y que traten de coordinar ambos bloques. Solo el art. 29.6 de la propuesta contiene una referencia al RGPD, cuando obliga a los usuarios de los sistemas de IA de alto riesgo a utilizar la información suministrada por el fabricante del sistema para llevar a cabo la evaluación de impacto exigida por el art. 35 RGPD. Por su parte, el art. 10 de la propuesta, titulado datos y gobernanza de datos, señala que los sistemas de alto riesgo que utilicen técnicas que implican el tratamiento de datos, deben desarrollarse a partir de datos que respeten prácticas adecuadas en materia de gobernanza y gestión de datos referidas en particular, a la elección de un diseño adecuado, la recopilación de datos, las operaciones de tratamiento para la preparación e datos, la formulación de los supuestos, la evaluación previa sobre la disponibilidad de la cantidad y adecuación de datos necesarios, el examen de posibles sesgos, la detección de lagunas o deficiencias. Señala, además, que los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes y representativos. Asimismo, cuando sea necesario los sistemas de alto riesgo podrán tratar categorías especiales de datos, con las salvaguardias necesarias para el respeto de los derechos y libertades fundamentales, entre esta incluye la posibilidad de establecer limitaciones técnicas a la reutilización de datos, tales como la seudonimización o el cifrado

Cabe apreciar una suerte de fragmentación entre, por un lado, las obligaciones de los fabricantes de sistemas de IA, centradas en garantizar la seguridad y, por otro lado, las obligaciones en materia de protección de datos que parecen incumbir únicamente al usuario final.

Esta rígida separación entre la normativa de protección de datos y la de IA determina que, cuando el sistema de IA comporte el tratamiento de datos, el empresario, como usuario del sistema, adquiera la condición de responsable del tratamiento de datos y sea el principal obligado por la normativa de protección de datos. Estas obligaciones

variarán según las utilidades del sistema de IA, el tipo de datos que se traten y la finalidad que se persiga.

Con carácter general, ha de recordarse que el RGPD se aplica exclusivamente cuando exista tratamiento de datos personales, no, por tanto, cuando los datos que se manejen no tengan tal entidad. Habrá por lo tanto supuestos en los que los sistemas de IA incorporados por el empresario no recopilen datos personales, sino, por ejemplo, datos sobre funcionamiento y rendimiento de la maquinaria, sobre la calidad del proceso de producción o de los propios productos, etc. Habrá, no obstante, otros casos en los que sí exista el citado tratamiento, lo cual obliga a respetar los principios y obligaciones específicas requeridas por el RGPD.

En una aproximación muy genérica, cabe recordar que el RGPD pivota sobre los principios de licitud, lealtad y transparencia, que determinan la necesidad de justificar el tratamiento de datos por alguna de las bases jurídicas previstas en el art. 6 RGPD y en garantizar su utilización para tal fin

En general, en el ámbito laboral, podrá justificarse la necesidad del tratamiento por motivos relacionados con la ejecución del contrato o con el cumplimiento de una obligación legal o en la existencia de un interés legítimo del interesado. Tal y como se ha señalado los sistemas de IA pueden permitir al empresario el acceso a un amplio volumen de información sobre la forma en que se desarrolla la prestación de trabajo y sobre los propios trabajadores, que pueden hallar justificación en motivos tales como la necesidad de supervisar y controlar la actividad laboral, necesidades de organización y dirección o en el cumplimiento de obligaciones específicas en materia de prevención. Será necesario analizar en cada caso si concurre la base legítima para el tratamiento[12]. Una vez acreditada la necesidad del tratamiento, el empresario ha de asegurar el cumplimiento del resto de principios en materia de protección de datos que

[12] Vid.: Baz Rodríguez (2019), J.: *Privacidad y protección de datos de los trabajadores en el entorno digital,* Wolters Kluwer; Goñi Sein, J.L. (2018): *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018),* Bomarzo.

le exigen garantizar los derechos del interesado entre los cuales están los de información, rectificación, supresión, limitación del tratamiento y oposición.

En orden a asegurar el cumplimiento de estos principios generales, el RGPD desgrana en sus artículos 24 y siguientes toda una serie de obligaciones que han de ser observadas por el responsable del tratamiento, en nuestro caso el empresario. Así se obliga a adoptar las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento es conforme con el RGPD. En concreto se le obliga a adoptar medidas desde el diseño, entre las que figuran la seudonimización, la minimización. Asimismo, se señala que entre las medidas técnicas y organizativas figura el seguimiento de políticas de protección de datos y la adhesión a códigos de conducta o mecanismo de certificación.

El RGPD exige, por último, la realización de una evaluación de impacto, cuando, con carácter general, el tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas y, en particular, cuando suponga una evaluación sistemática de aspectos personales que se base en tratamiento automatizado o en la elaboración de perfiles sobre cuya base se tomen decisiones con efectos jurídicos. La Agencia Española de Protección de Datos, como autoridad de control, ha elaborado una lista indicativa de tratamientos de datos que exigirían tal evaluación en la que figuran los tratamientos que impliquen perfilado o valoración de sujetos en ámbitos de su vida como el desempeño en el trabajo, tratamientos que impliquen toma de decisiones automatizadas, tratamientos que implique la observación, monitorización, supervisión, geolocalización[13].

Se observa, por tanto, cómo el empresario se erige en el máximo garante del cumplimiento de los principios de protección de datos. Existen, sin embargo, tal y como se señalaba, momentos en los que quizás no sea el empresario quien se encuentre en mejor posición para asegurar el cumplimiento de tales principios. Así, por ejemplo, el fabricante del sistema IA puede encontrarse en una situación más adecuada para garantizar el tratamiento de los datos

[13] https://www.aepd.es/es/documento/listas-dpia-es-35-4.pdf

para las estrictas funcionalidades del sistema de IA, garantizando cuando fuera posible la anonimización. Igualmente, el propio fabricante podría estar en mejor posición para arbitrar desde el mismo diseño mecanismos que permitieran un fácil ejercicio de derechos como los de acceso y rectificación.

Igualmente, habrá ocasiones, en las que el fabricante del sistema IA puede ayudar al empresario al cumplimiento de sus obligaciones y, en consecuencia, hubiera sido deseable la imposición de ciertas obligaciones específicas, principalmente de información, al citado fabricante. Así, el diseñador del sistema IA puede ayudar al empresario en el cumplimiento del deber de transparencia, facilitando en un lenguaje sencillo información sobre los datos que se recogen, el modo de recogida, el tratamiento y su finalidad. También el fabricante podría suministrar información valiosa sobre el funcionamiento del sistema de IA y sus posibles aplicaciones, en orden a determinar si se está ante un sistema que encaje en alguno de los supuestos de tratamiento de datos que requiere evaluación de impacto.

Así ha sido puesto de manifiesto explícitamente en su informe sobre la propuesta por la Agencia Europea de Protección de Datos y por el supervisor Europeo de Protección de datos. En línea con lo señalado en este informe existen diferentes ámbitos y momentos concretos dentro del proceso de fabricación y utilización de sistemas de IA en los que tanto la normativa de IA, como la de protección de datos deberían interactuar de forma explícita.

No se ha tratado en la propuesta de integrar ya en el diseño y fabricación de los sistemas de IA los principios que presiden la normativa en materia de protección de datos. Hubiera sido interesante, por ejemplo, que en la propuesta de ley se impusiera al fabricante de sistemas de IA obligaciones con el fin de que desde el diseño se evitara el tratamiento de datos innecesarios, se incorporasen al sistema mecanismos que permitieran el ejercicio de derechos como el de cancelación o corrección.

Asimismo, también hubiera sido factible que el fabricante realizara una evaluación de riesgos del sistema teniendo en cuenta los posibles usos a los que se destine, lo cual a su vez

podría ayudar al usuario final en su propia evaluación[14]. En efecto, tanto la propuesta de ley de IA como la normativa en materia de protección de datos han previsto sus propios mecanismos de evaluación y acreditación de la conformidad. Así, tal y como se ha visto, la propuesta de ley de IA, exige que los productos de alto riesgo se sometan a una evaluación por tercero. Por su parte, el RGPD exige también en determinadas ocasiones una evaluación de impacto. Teniendo en cuenta este marco normativo hubiera sido oportuno prever un procedimiento de evaluación que sirviera para ambos propósitos, sin embargo, no ha sido así, el marcado CE previsto en la propuesta de ley de IA servirá para acreditar la conformidad con tal propuesta, pero no exime de la posible de la realización de la evaluación de impacto adicional en caso de que se den los requisitos previstos en el RGPD.

6. APROXIMACIÓN A LA NUEVA NORMATIVA EN MATERIA DE RESPONSABILIDAD CIVIL DERIVADA DE PRODUCTOS DEFECTUOSOS Y POR DAÑOS CAUSADOS POR SISTEMAS DE IA

Cuando el trabajador sufra un daño como consecuencia de la utilización de un producto que incorpora un sistema de IA o de un sistema de IA autónomo, podrá reclamar la indemnización correspondiente, destinada al resarcimiento de tales daños.

La exigencia con que la LPRL, en su art. 14, configura la obligación de seguridad del empresario, determina que en buena parte de los supuestos el empresario asuma la responsabilidad civil derivada de daños causados al trabajador. Junto a ello, existe la posibilidad de que también haya de hacer frente a una eventual responsabilidad administrativa o penal y al recargo de prestaciones.

[14] Así lo han puesto de manifiesto el EDPD-EDPS en su comunicado conjunto. EDPB-EDPS. Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 18 de junio de 2021, disponible en https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

Con todo, ha de tenerse en cuenta que en el ámbito específico de la responsabilidad civil por productos defectuosos existe un régimen particular, armonizado a nivel europeo, que está siendo objeto de revisión. Asimismo, se está avanzando en una norma específica para reparar los daños causados por sistemas de IA[15].

En lo que se refiere a la normativa de responsabilidad por productos defectuosos, se ha aprobado el pasado 28 de septiembre de 2022, la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos[16]. De forma simultánea, el mismo día, vio la luz la Propuesta de Directiva de Parlamento Europeo y del Consejo, relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA)[17].

Con carácter general, la Directiva sobre responsabilidad por productos defectuosos, que en caso de aprobación derogará la actual Directiva 85/374, trata de acomodar esta normativa vigente para dar respuesta a algunos de los problemas que suscitan la aparición como productos de estos sistemas de IA. Para ello, procede, en primer lugar, a acomodar la definición de producto a los nuevos desarrollos derivados de la IA. Así, el art. 4.1 de la propuesta define como producto: "cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble; por producto se entiende también (…) los archivos de fabricación digital y los programas informáticos". Se incluye, por tanto, expresamente como producto a los programas informáticos.

El apartado 3 del mismo artículo define como componente: "cualquier artículo, tangible o intangible o cualquier servicio conexo que está integrado en un producto o interconectado

[15] EGUSQUIZA BALMASEDA, M.A.: "Marco normativo general y propuestas de regulación en la responsabilidad civil" en AA.VV. (EGUSQUIZA BALMASEDA, M.A y RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* op. cit. Vid. también en la misma obra: JORQUI AZOFRA, M.: "El concepto legal de producto a la luz de la nueva propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos".

[16] COM 2022/0302

[17] COM 2022 (496) final

con él por el fabricante de ese producto o que esté bajo su control". Por último, el servicio conexo es definido en el apartado 4 como: "un servicio digital que está integrado en un producto o interconectado con él, de tal manera que su ausencia impediría al producto realizar una o varias de sus funciones".

El art. 7 de la propuesta obliga a los Estados a garantizar que el fabricante de un producto defectuoso pueda ser considerado responsable de aquellos daños causados por ese producto y se añade que, cuando un componente defectuoso haya provocado que el producto sea defectuoso, el fabricante de ese componente también puede ser considerado responsable de los daños.

De lo anterior cabe deducir que el fabricante de un sistema de IA, comercializado de forma autónoma, podrá ser considerado responsable con base en la Directiva, gracias a la inclusión expresa en la definición de producto de los sistemas de IA autónomos.

Asimismo, el fabricante de un equipo que incorpore un sistema de IA también podrá considerarse responsable de los posibles daños, cuando sea considerado defectuoso.

El fabricante que incorpore un componente o un servicio conexo bajo su control también será considerado responsable. Junto a él, el fabricante del componente o servicio conexo que ha causado el defecto, también podrá ser considerado responsable solidario.

Por último, el art. 7.4 señala que cualquier persona física o jurídica que modifique un producto se considerará fabricante, cuando la modificación sea sustancial. De tal manera que, en los casos en los que el empresario realiza alteraciones sustanciales del equipo será considerado fabricante, y posible sujeto responsable, a los efectos de la Directiva. No se consideran modificaciones sustanciales las simples actualizaciones o mejoras del producto realizadas bajo el control del fabricante.

A partir de aquí, la Directiva trata de facilitar la carga de la prueba del perjudicado, de tal manera que basta con que pruebe el carácter defectuoso del producto, los daños sufridos y el nexo causal. Con el fin de facilitar el carácter defectuoso del producto se faculta a los órganos

jurisdiccionales nacionales a que, cuando el demandante haya presentado pruebas suficientes de la posible existencia del defecto, reclamen la exhibición de pruebas necesarias para valorar la existencia del defecto (art. 8 y 9 de la propuesta).

Conforme a este régimen se pueden reclamar los daños derivados de muerte o lesiones corporales, incluidos los daños psicológicos, los daños derivados de la pérdida o corrupción de datos que no se utilicen con fines profesionales y los daños en cualquier propiedad, salvo en el propio producto defectuoso y en propiedades utilizadas con fines profesionales

De forma paralela, tal y como se ha apuntado, la UE ha impulsado la Directiva sobre responsabilidad en materia de IA. Esta Directiva, tal y como reconoce en su art. 1.3 b) no afecta a los posibles derechos que asistan a los perjudicados en virtud de la Directiva de productos defectuosos, que se acaba de analizar. El objeto de la Directiva es establecer normas comunes sobre todo en materia de carga de la prueba para las demandas de responsabilidad civil extracontractual subjetiva por daños y perjuicios causados por sistemas de IA. Se trata, por tanto, de una norma que se basa en la prueba de la culpa, no del defecto, pero que trata de facilitar dicha prueba.

Con carácter general, el art. 4,1 señala que se presumirá el nexo causal entre la culpa y los resultados producidos por el sistema de IA cuando se den las siguientes condiciones: que se haya probado el incumplimiento de un deber de diligencia, que pueda considerarse razonablemente probable que la culpa ha influido en los resultados producidos por el sistema de IA, que la información de salida producida por el sistema de IA causó los daños.

En el caso de los sistemas de IA de alto riesgo se entiende que se cumple el requisito de no observación del deber de diligencia cuando no se hayan observado las obligaciones recogidas en los capítulos 2 y 3 del proyecto de Ley de IA. Se establecen, además, una serie de obligaciones para el proveedor de un sistema de IA de alto riesgo, consistentes en la aportación de pruebas sobre el sistema de IA del que se sospecha que ha causado un daño, siempre que el

demandante haya aportado indicios suficientes sobre la viabilidad de la demanda (art. 3). No obstante, se señala que no se aplicará la presunción cuando el demandado demuestre que el demandante puede acceder razonablemente a pruebas que demuestran el nexo de causalidad (art. 4.4). En el caso de sistemas de IA que no son de alto riesgo la presunción solo se aplicará cuando el órgano judicial considere excesivamente difícil para el demandante demostrar el nexo causal (art.4.5).

Por último, esta norma incorpora la previsión de posibles demandas por daños contra los usuarios de sistemas de IA de alto riesgo que, en el caso de equipos destinados al ámbito laboral, podrían ser los empresarios. En estos casos se entenderá que no ha observado el deber de diligencia cuando no haya cumplido las obligaciones previstas en el art. 29, en concreto, no cumplir con sus obligaciones de utilizar o supervisar el sistema de IA de conformidad con las instrucciones, o haber expuesto al sistema a datos de entrada bajo su control que no eran pertinentes (art.4.3).

7. BIBLIOGRAFÍA

EU-OSHA: *Advanced robotics and automation: implications for occupationl safety and health,* 2022, disponible en: https://osha.europa.eu/en/publications/advanced-robotics-and-automation-implications-occupational-safety-and-health

EU-OSHA: *Artificial intelligence for worker management: an overview,* 2022, disponible en https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-overview

EU-OSHA: *Artificial intelligence for worker management: mapping definitions, uses and implications,* 2022, disponible en: https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-mapping-definitions-uses-and-implications

GOÑI SEIN, J.L.: Ley de inteligencia artificial y seguridad y salud en el trabajo", en AA.VV. (dir.: Rodríguez Sanz de Galdeano, B. y Egusquiza Balmaseda, M.A.: *Inteligencia artificial y prevención de riesgos*

laborales: obligaciones y responsabilidades, Tirant lo Blanch, 2023, en prensa.

BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital,* Wolters Kluwer, Madrid, 2019.

GOÑI SEIN, J.L.: *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018),* Bomarzo, 2018.

EGUSQUIZA BALMASEDA, M.A.: "Marco normativo general y propuestas de regulación en la responsabilidad civil" en AA.VV. (EGUSQUIZA BALMASEDA, M.A y RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.

JORQUI AZOFRA, M.: "El concepto legal de producto a la luz de la nueva propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos" en AA.VV. (EGUSQUIZA BALMASEDA, M.A y RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.