

**TRABAJO FIN DE ESTUDIOS / IKASGAIEN AMAIERAKO LANA**  
**MÁSTER UNIVERSITARIO EN PREVENCIÓN DE RIESGOS LABORALES**

.....

**INTELIGENCIA ARTIFICIAL Y PREVENCIÓN DE RIESGOS LABORALES**

**Arantxa Goñi Erro**

**DIRECTOR / ZUZENDARIA**

**Julen Llorens Espada**

**Pamplona / Iruñea**

**18 de enero de 2024**

## **Resumen**

El objetivo del presente estudio es analizar la categorización de sistemas IA aplicables a Prevención de Riesgos Laborales, atendiendo a la Ley de Inteligencia Artificial. Para ello, se analiza la categorización, en función del riesgo, propuesta por la Comisión Europea, así como los distintos requisitos establecidos en cada una de estas categorías. Posteriormente, con base en dichos requisitos, se analiza la categorización de distintos sistemas y aplicaciones IA del ámbito de la seguridad y salud en el trabajo. Asimismo, se analizan los requisitos y obligaciones que pudieran derivar para las distintas partes implicadas en el uso de este tipo de sistemas, así como las posibles consecuencias que su uso pudiera tener en las personas trabajadoras.

**Palabras clave:** Inteligencia Artificial, Riesgo, Discriminación, Seguridad, Salud.

## **Abstract**

This study aims to analyze the categorization of AI systems applicable to Occupational Health and Safety, according to the Artificial Intelligence Law. For this purpose, the categorization, according to risk, proposed by the European Commission is analyzed, as well as the different requirements established in each of these categories. Subsequently, based on these requirements, the categorization of different AI systems and applications in the field of Occupational Health and Safety is analyzed. It also analyzes the requirements and obligations that may arise for the different parties involved in the use of such systems, as well as the possible consequences that their use may have on employees.

**Key words:** Artificial Intelligence, Risk, Discrimination, Safety, Health.

# Índice

|   |    |
|---|----|
| <b>I. INTRODUCCIÓN</b> .....  | 4  |
| <b>II. REGLAMENTO INTELIGENCIA ARTIFICIAL</b> .....                                 | 5  |
| <b>1. Clasificación del riesgo</b> .....  | 8  |
| 1.1. <i>Riesgo inadmisibile o prácticas prohibidas</i> .....                        | 9  |
| 1.2. <i>Alto riesgo</i> .....   | 10 |
| 1.3. <i>Riesgo limitado</i> .....   | 12 |
| 1.4. <i>Riesgo mínimo</i> .....   | 13 |
| <b>III. LA IA APLICADA A LA PREVENCIÓN DE RIESGOS LABORALES</b> .....               | 14 |
| <b>2. Prácticas de inteligencia artificial prohibidas</b> .....                     | 15 |
| <b>3. Prácticas de inteligencia artificial de alto riesgo</b> .....                 | 21 |
| 3.1. <i>EPIs inteligentes</i> .....   | 26 |
| 3.2. <i>Software de gestión preventiva (AIWM)</i> .....                             | 27 |
| 3.3. <i>Trabajo en plataformas digitales</i> .....                                  | 29 |
| 3.4. <i>Requisitos de los sistemas de alto riesgo y obligaciones</i> .....          | 30 |
| <b>4. Sistemas de Inteligencia Artificial de riesgo limitado y mínimo</b> .....     | 33 |
| <b>IV. OBLIGACIONES DEL USUARIO O EMPLEADOR</b> .....                               | 35 |
| <b>V. POSIBLES IMPACTOS NEGATIVOS DEL USO DE SISTEMAS DE IA EN EL TRABAJO</b> ..... | 37 |
| <b>VI. CONCLUSIONES</b> .....   | 39 |
| <b>VII. BIBLIOGRAFÍA</b> .....  | 43 |

## I. INTRODUCCIÓN

A pesar de que el término “Inteligencia Artificial surge en el año 1956, no ha sido hasta principios del siglo XXI cuando la IA ha entrado con fuerza en escena. Tal es así que esta figura y, por derivación, los algoritmos cada día están en más ámbitos, incluido el laboral, donde su influencia no deja de crecer<sup>1</sup>. De acuerdo con algunos registros disponibles en España, comparando la situación de 2021 con la de 2022, de un año para otro el uso de la IA por las empresas ha crecido hasta el 11,8%<sup>2</sup>.

Comúnmente, a esta transición se la conoce como “cuarta revolución industrial”., lo que probablemente, en similitud a las tres revoluciones industriales anteriores, traerá grandes cambios no solo en las personas, sino también en las empresas. Cada una de dichas “revoluciones industriales” ha traído nuevos cambios, como ejemplo de cada una de ellas, en el siglo XIX con la máquina de vapor, en el Siglo XX la electricidad y la tercera, incorporando, entre otras, una mayor utilización de las energías renovables<sup>3</sup>.

Actualmente, la cuarta revolución industrial es caracterizada por la “industria 4.0” y la incorporación de nuevas tecnologías, como el internet de las cosas (IoT), análisis y cloud computing, IA y machine learning<sup>4</sup>. Sin embargo, la introducción de este tipo de herramientas puede implicar resultados sesgados o discriminatorios, planteando cuestiones éticas y humanas que deben ser abordadas para asegurar un uso responsable<sup>5</sup>.

A pesar de que la IA puede llegar a tener gran impacto a nivel empresarial, son muchas las áreas en las que este tipo de sistemas están siendo integrados. Conscientes de los múltiples usos, beneficios y desafíos que este nuevo paradigma plantea en la Unión Europea, en los últimos años se ha desarrollado el “Reglamento de Inteligencia Artificial”, con objeto de garantizar que los sistemas de IA utilizados en la UE sean seguros y respetes los derechos fundamentales y valores de la UE.

---

<sup>1</sup>MEGINO FERNÁNDEZ, Diego. “La formación como principio y fin de la acción preventiva frente a los riesgos psicosociales derivados de la digitalización y la automatización” en *Lan Harremanak-Revista de Relaciones Laborales*, núm 49, 2023, págs. 115-154

<sup>2</sup> Observatorio Nacional de Tecnología y Sociedad (2023) “Uso de inteligencia artificial y big data en las empresas españolas”, 2023.

<sup>3</sup> SALGUERO-CAPARRÓS, Francisco Miguel, “Seguridad laboral e industrial: nuevas tecnologías en la Industria 4.0”. Universidad de Málaga

<sup>4</sup> IBM, Cómo las tecnologías de la Industria 4.0 están cambiando la fabricación. <https://www.ibm.com/es-es/topics/industry-4-0>

<sup>5</sup> TAPIA CEDEÑO, STEFANÍA JOHANNA. “La inteligencia artificial como herramienta complementaria en la investigación y educación: responsabilidad ética y humana” en *Revista Unidad Sanitaria XXI*, 3(8).

A pesar de que, como más adelante veremos, el Reglamento no analiza de forma concreta la aplicación de los sistemas IA en prevención de riesgos laborales, este también es uno de los ámbitos en el que este tipo de sistemas pueden ser utilizados. De esta forma, a pesar de que son diversas las formas en las que la IA puede ser integrada en aspectos de seguridad y salud en el trabajo (EPIs inteligentes, robots colaborativos, exoesqueletos industriales, etc.), esta integración se debe hacer respetando los nuevos límites y obligaciones establecidas por el Reglamento IA.

Siendo esto así, el presente trabajo tiene como objetivo analizar el Reglamento de IA, para determinar el tipo de herramientas o sistemas que pudieran encajar en cada una de las disposiciones previstas en el Reglamento.

## II. REGLAMENTO INTELIGENCIA ARTIFICIAL

La inteligencia artificial cada vez tiene mayor presencia en nuestro día a día, así como en el día a día de empresas de diversos sectores. A pesar de ello, esta misma herramienta que es capaz de generar grandes beneficios, da lugar a nuevos riesgos o consecuencias negativas. Siendo esto así, y en vista de la velocidad a la que se desarrolla la tecnología y las dificultades que podrían surgir, la Unión Europea ha desarrollado la Ley de Inteligencia Artificial, con el objetivo de que los ciudadanos de la Unión Europea puedan aprovechar las nuevas tecnologías que se desarrollen y funcionen de acuerdo con los valores, los derechos fundamentales y los principios de la UE<sup>6</sup>.

El desarrollo legislativo sobre la Inteligencia Artificial comienza en 2018, con la Comunicación de la Comisión “Inteligencia artificial para Europa”, teniendo como objetivo convertir a la Unión Europea en motor en materia de Inteligencia Artificial, sin olvidar los valores éticos y jurídicos de esta. En esta, se propone una IA centrada en el ser humano, además de destacar la IA como herramienta para resolver importantes desafíos. Este mismo año, la Comisión crea un Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial, encargado de formular directrices sobre una IA fiable<sup>7</sup>.

---

<sup>6</sup> Reglamento (UE) nº 1169/2011 del Parlamento Europeo y del Consejo

<sup>7</sup> GOÑI SEIN, José Luis: "El Reglamento UE de Inteligencia Artificial y su interrelación con la normativa de seguridad y salud en el trabajo", en RODRÍGUEZ SANZ DE GALDEANO, Beatriz y EGÚSQUIZA BALMASEDA, M<sup>a</sup> Ángeles (dir.): *Obligaciones y responsabilidades*. Tirant lo Blanch, Valencia, 2023, págs. 73-119

Le sigue en 2020 el “Libro Blanco sobre Inteligencia Artificial”, donde se sientan las bases de la propuesta de Reglamento. En este, se plantea un enfoque orientado a la excelencia y la confianza, ya que se argumenta que, entre muchas otras cosas, el rápido desarrollo de la inteligencia artificial mejorará la atención sanitaria, aumentará la eficiencia de la agricultura y contribuirá a la mitigación del cambio climático. Asimismo, se persigue acercar las ventajas de la tecnología a la sociedad y la economía europea en su conjunto, haciendo partícipes a los ciudadanos, el desarrollo empresarial y los servicios de interés públicos.

Este mismo año, se publica el “Informe sobre repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica”, en el que se concluye que la legislación vigente en materia de seguridad de los productos presenta algunas deficiencias que deben subsanarse en la Directiva de máquinas<sup>8</sup>.

Finalmente, en 2021, la Comisión Europea publica el borrador de la propuesta de Reglamento sobre Inteligencia Artificial. Este se desarrolla teniendo como base los valores y derechos fundamentales de la UE<sup>9</sup>, además de asegurar un desarrollo normativo suficiente que no supusiera una carga excesiva para el desarrollo de las innovaciones tecnológicas<sup>10</sup>. Es decir, entre otros, se persigue garantizar que el desarrollo, la comercialización y el uso de los sistemas de IA en el mercado de la UE sean seguros, fiables y respeten la legislación vigente en materia de derechos fundamentales y valores de la UE.

Respecto a la creación de una IA confiable, la Comisión ha impulsado tres iniciativas jurídicas. En primer lugar, creación de un marco jurídico europeo para la IA con el que se busca aportar seguridad jurídica a los desarrolladores, implementadores y usuarios de IA, estableciendo unos requisitos y obligaciones específicos. Fruto de esta nace en 2021 la propuesta de Reglamento IA anteriormente mencionado.

En segundo lugar, un marco jurídico europeo común para la responsabilidad civil que pueda surgir de daños generados por el uso de Inteligencia Artificial, la cual se ve cubierta a través de la Directiva sobre responsabilidad en materia de IA. En tercer lugar, la

---

<sup>8</sup>RODRÍGUEZ SANZ DE GALDEANO, Beatriz: " Los sistemas de inteligencia artificial en el ámbito laboral y el marco regulador europeo de seguridad del producto", en RODRÍGUEZ SANZ DE GALDEANO, Beatriz y EGÚSQUIZA BALMASEDA, M<sup>a</sup> Ángeles (dir.): *Obligaciones y responsabilidades*. Tirant lo Blanch, Valencia, 2023, págs. 23-69

<sup>9</sup> Reglamento (UE) n° 1169/2011 del Parlamento Europeo y del Consejo

<sup>10</sup> RODRÍGUEZ SANZ DE GALDEANO, Beatriz (2023). Op Cit. pag.34

Comisión plantea la necesidad de adaptar este nuevo marco a la normativa relativa sobre seguridad del producto, de forma que se propone un nuevo Reglamento junto con el de responsabilidad para productos defectuosos.

Además de esto, los objetivos específicos marcados por la Comisión son los siguientes<sup>11</sup>:

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

Para lograr tales objetivos, la propuesta declara sustentarse en un enfoque regulador horizontal equilibrado y proporcionado, circunscrito a los requisitos mínimos necesarios para abordar los riesgos y problemas vinculados a la IA, sin limitar ni obstaculizar indebidamente el desarrollo tecnológico ni aumentar de forma desproporcionada el coste de la comercialización de las soluciones de IA<sup>12</sup>.

Cabe destacar que esta regulación adquiere forma de Reglamento, no de Directiva. De esta forma, el texto adquiere eficacia vinculante para todos los estados miembros desde su entrada en vigor, sin necesidad de transposición al derecho interno. Asimismo, el Reglamento establece en su artículo 2 que será de aplicación a todos los proveedores que comercialicen o pongan en servicio sistemas de IA en la Unión, independientemente de que dichos proveedores estén o no establecidos en la Unión<sup>13</sup>.

---

<sup>11</sup> Reglamento (UE) n° 1169/2011 del Parlamento Europeo y del Consejo

<sup>12</sup> GAMERO CASADO, Eduardo. "El enfoque europeo de Inteligencia Artificial" en *Revista de Derecho Administrativo*, núm. 20, 2021, págs. 268-289

<sup>13</sup> GAMERO CASADO, Eduardo (2021) Op. Cit pag.277

## 1. Clasificación del riesgo

Antes de comenzar a analizar la categorización aplicada por el Reglamento, es importante comprender qué se entiende por Sistema de Inteligencia Artificial, ya que la definición legalmente establecida será la que limite el ámbito de aplicación. Es importante tener en cuenta que la Comisión se enfrenta a un reto, es crucial establecer una definición que sea lo suficientemente precisa, de forma que limite de forma correcta el ámbito de aplicación, pero a su vez, esta debe ser lo suficientemente flexible para tener la capacidad de adaptarse a la evolución de la tecnología<sup>14</sup>.

Esto ha supuesto un reto y ya existe una modificación de la definición inicialmente planteada. La primera definición establecida hacía referencia a *“el software que desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa”* (Artículo 3 Reglamento IA).

Posteriormente, dicha definición de Sistema de Inteligencia Artificial se modifica por *“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”* (Artículo 3 Reglamento IA).

Dicho esto, el Reglamento sigue un enfoque basado en los riesgos para la seguridad y los derechos fundamentales, distinguiendo así cuatro niveles: Riesgo inadmisibles o prácticas prohibidas, alto riesgo, riesgo limitado y riesgo mínimo. Siendo esto así, no todos los sistemas de IA estarán sujetos a las mismas reglas, sino que esto variará en función del nivel de alcance que la aplicación de IA pueda generar, de forma que cuanto mayor es el riesgo, más estrictas son las reglas.<sup>15</sup>

---

<sup>14</sup> GAMERO CASADO, Eduardo (2021) Op. Cit pag.277

<sup>15</sup>Portal Administración Electrónica (2023) “Ley de Inteligencia Artificial: el Consejo y el Parlamento Europeo llegan a un acuerdo sobre las primeras normas para regular la IA en el mundo [https://administracionelectronica.gob.es/pae/Home/pae\\_Actualidad/pae\\_Noticias/Anio2023/Diciembre/Noticia-2023-12-11-Ley-de-inteligencia-artificial-el-Consejo-y-el-Parlamento-Europeo-llegan-a-un-acuerdo-sobre-las-primeras-normas-en-el-mundo-para-regular-la-Inteligencia-Artificial.html](https://administracionelectronica.gob.es/pae/Home/pae_Actualidad/pae_Noticias/Anio2023/Diciembre/Noticia-2023-12-11-Ley-de-inteligencia-artificial-el-Consejo-y-el-Parlamento-Europeo-llegan-a-un-acuerdo-sobre-las-primeras-normas-en-el-mundo-para-regular-la-Inteligencia-Artificial.html)

### *1.1. Riesgo inadmisibles o prácticas prohibidas*

El Reglamento comienza exponiendo las prácticas que, debido a la perjudicialidad y que pudieran llegar a suponer, son inadmisibles dentro de la UE. Estas, quedan recogidas en el título II del Reglamento y se refiere a aquellas prácticas de manipulación, explotación y control social, 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, como son el de la no discriminación, la protección de datos y la privacidad<sup>16</sup>.

Este tipo de prácticas engloba además aquellas que tienen un gran potencial para manipular a las personas, trascendencia su conciencia o aprovechando su vulnerabilidad (grupos vulnerables concretos, menores o las personas con discapacidad), para alterar de manera sustancial su comportamiento de modo que puede provocar perjuicio ya sea físico o psicológico a ellos mismos o a otras personas. Dichas limitaciones incluyen asimismo las neurotecnologías asistidas mediante sistemas de IA utilizadas para supervisar, utilizar o influir en los datos neuronales recopilados a través de interfaces cerebro-ordenador. Quedan igualmente prohibidos los sistemas de IA con capacidad de clasificar a las personas físicas, por considerarse especialmente intrusivos, vulnerar la dignidad humana y presentar un gran riesgo de discriminación

Asimismo, se prohíbe que las autoridades públicas realicen calificación social basada en IA con fines generales, así como el uso de sistemas de identificación biométrica remota “en tiempo real” en espacios de acceso público con fines de aplicación de la ley, ya que puede afectar a la vida privada de gran parte de la población, provocar la sensación de estar bajo control constante y otorgar una posición de poder incontrolable a quien los aplica<sup>17</sup>. Los sistemas de identificación biométrica remota “en diferido” se prohibirán en espacios públicos, a menos que, exista autorización judicial previa para su uso en el contexto de la aplicación de la ley, cuando sea estrictamente necesario para la investigación de delito grave.

En lo que al ámbito laboral respecta, interesan concretamente las prácticas de IA de manipulación, explotación y control social, así como aquellas que vayan en contra de los valores de la Unión y los Derechos Fundamentales por esta reconocidos y el uso de datos

---

<sup>16</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 84

<sup>17</sup> Reglamento (UE) nº 1169/2011 del Parlamento Europeo y del Consejo

biométricos. Son especialmente preocupantes los sistemas de IA que procuran la detección de emociones, los rasgos físicos o psicológicos, movimientos, frecuencia cardiaca o voz. Estos sistemas son de limitada fiabilidad y por los problemas que pudieran derivar, se prohíbe la introducción al mercado, puesta en servicio y el uso de sistemas de sistemas de IA diseñados para utilizarse en el lugar de trabajo, entre otros, a fin de detectar el estado emocional de las personas físicas (Considerando 9).

### *1.2. Alto riesgo*

Quedan recogidas en el título III y en este caso, son aquellos sistemas que puedan suponer un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas. Estos sistemas, a diferencia de los anteriores, sí están permitidos en el mercado, siempre que cumplan con determinados requisitos obligatorios que más adelante se detallan y sean sometidos a una evaluación de conformidad ex ante.

En el capítulo 1 del título III, concretamente en el artículo 6.2, se establecen las normas de clasificación y se definen dos subcategorías principales de sistemas de IA de alto riesgo:

- Sistemas de IA diseñados para utilizarse como componentes de seguridad de productos sujetos a una evaluación de conformidad previa realizada por terceros
- Otros sistemas de IA independientes no incorporados a otros productos específicos. Se indican en el Anexo III y se establecen en este debido a que los sistemas que aparecen en este implican riesgos que ya se han materializado o que es probable que lo hagan próximamente. El Anexo III hace concretamente referencia a<sup>18</sup>:
  1. Identificación biométrica remota de personas a tiempo real o a distancia, a excepción de la condición anteriormente mencionada entre las prácticas inadmisibles.
  2. Gestión y funcionamiento de infraestructuras críticas
  3. Educación y formación profesional
  4. El empleo, la gestión de los trabajadores y el acceso al autoempleo
  5. Acceso y disfrute de servicios privados y públicos privados y públicos y ayudas públicas esenciales

---

<sup>18</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 87

6. Aplicación de la ley
7. Gestión de la migración, asilo y control fronterizo
8. Administración de justicia y procesos democráticos

Entre estas, a nivel laboral nos interesan especialmente los puntos uno (*Identificación biométrica remota de personas a tiempo real o a distancia, a excepción de la condición anteriormente mencionada entre las prácticas inadmisibles*) y cuatro (*El empleo, la gestión de los trabajadores y el acceso al autoempleo*). Los sistemas aplicados en estos ámbitos pueden perpetuar patrones de discriminación, pudiendo perjudicar los derechos fundamentales. Antes de la puesta en servicio o del uso de un sistema de este tipo en el lugar de trabajo, se deberá consultar a los representantes de los trabajadores, así como informar al personal que estará expuesto (Artículo 29, apartado 5 bis).

Siendo esto así, las aplicaciones de IA que se encuentren dentro de esta categoría deberán cumplir una serie de requisitos obligatorios, de forma que se asegure que estas no entrañen riesgos inaceptables. Asimismo, el empresario que pretenda implementar este tipo de sistemas, tengan o no un impacto perjudicial importante, se deberán integrar teniendo en cuenta tanto la Ley de Protección de Datos Personales como la Ley de Prevención de Riesgos Laborales.

Entrando a definir las obligaciones a las que los sistemas de IA de alto riesgo están sujetas, se centran especialmente en la fase previa a la comercialización de dichos sistemas, siendo requisito esencial y bajo responsabilidad del proveedor la realización de una evaluación de conformidad antes de introducir el sistema al mercado<sup>19</sup>. Dicha evaluación de conformidad será obligatoria en los supuestos establecidos en el artículo 43.1 de la Ley IA, mediante la cual el proveedor que quiera comercializar sistemas de IA acredite el cumplimiento de los requisitos obligatorios<sup>20</sup>:

- Sistema de gestión de riesgos (art. 9), así como el mantenimiento de este durante todo el ciclo de vida del sistema. Esto implica identificar los riesgos conocidos y previsibles, evaluar los riesgos y adoptar las medidas oportunas de eliminación, reducción de riesgos asociados a la utilización del sistema y comprobación del funcionamiento de modo adecuado a la finalidad prevista<sup>21</sup>.

---

<sup>19</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 90

<sup>20</sup> Comisión Europea (2022) "Propuesta de marco normativo sobre inteligencia artificial" <https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai>

<sup>21</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 90

- Datos y gobernanza de datos (art. 10)
- Documentación técnica (art. 11)
- Registros (art. 12)
- Transparencia y comunicación de información a los usuarios (Art. 13)
- Vigilancia humana (art. 14)
- Precisión, solidez y ciberseguridad (Art. 15)

Desde el punto de vista de las obligaciones a nivel empresarial, el empresario toma la misma posición que el resto de los usuarios de sistemas de IA, de forma que se le atribuyen las mismas obligaciones que al resto, establecidas en el artículo 29 de esta misma Ley. Ante esta lista de obligaciones, es importante tener en cuenta que, aunque esta ley el empresario no asume obligaciones adicionales, el art 29.2 establece que estas obligaciones “*deben entenderse sin perjuicio de otras obligaciones que el Derecho de la Unión o nacional impongan a los usuarios*”. Siendo esto así, el empresario que ponga a disposición de las personas trabajadoras sistemas de IA que puedan clasificarse como de Alto Riesgo, deberá asegurarse de cumplir asimismo la Directiva Marco en materia de seguridad y salud en el trabajo, entre otras<sup>22</sup>. Por último, las personas que implementen estos sistemas deberán conservar, durante un periodo mínimo de seis meses, los archivos de registro que sean necesarios para garantizar el cumplimiento de las obligaciones legalmente establecidas<sup>23</sup>.

### *1.3. Riesgo limitado*

En tercer lugar, el riesgo limitado queda recogido en el título IV y se refiere a aquellos cumplan alguno de los tres requisitos a continuación mencionados; Están destinados a interactuar con personas físicas, son sistemas de reconocimiento de emociones o de categorización biométrica en cuanto al funcionamiento de los mismos o sistemas que generen manipulación de imágenes y sonidos y que puedan inducir erróneamente a una persona a pensar que son auténticos o verídicos (ultrafalsificaciones)<sup>24</sup>.

Estas prácticas están sujetas a obligaciones de transparencia, de forma que cuando el usuario o usuaria interactúe con un sistema de IA o sus emociones o características sean

---

<sup>22</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 93

<sup>23</sup> Artículo 29, apartado 5, párrafo 1 Reglamento IA

<sup>24</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 110

reconocidas por medios automatizados, la persona deberá ser informada de tal circunstancia.

Del mismo modo, cuando un contenido audiovisual generado por IA pueda confundirse con contenido auténtico, debe ser obligatorio informar de que dicho contenido ha sido generado por medios automatizados<sup>25</sup>. Del mismo modo, en caso de que el empresario ponga a disposición sistemas de IA considerados de riesgo limitado, deberá realizar una evaluación del impacto de los riesgos residuales sobre la protección de datos y la seguridad y salud del trabajador desde la perspectiva de prevención de riesgos laborales<sup>26</sup>.

#### *1.4. Riesgo mínimo*

El último lugar, el resto de los sistemas quedan recogidos en el título IX. Estos sistemas pueden desarrollarse y utilizarse bajo la legislación vigente sin obligaciones jurídicas adicionales<sup>27</sup>.

Este tipo de sistemas son considerados por parte del legislador como los más comunes y únicamente sugiere la voluntariedad por parte de los proveedores de crear o adherirse a códigos de conducta (los mismos obligatorios para sistemas de alto riesgo)<sup>28</sup>. Asimismo, se añade la voluntariedad de incluir en dicho código otros compromisos voluntarios, como pueden ser la sostenibilidad medioambiental, la accesibilidad para las personas con discapacidad, la participación de las partes interesadas en el diseño y el desarrollo de sistemas de IA, y la diversidad de los equipos de desarrollo<sup>29</sup>.

A esto se le añade que, igual que en el caso de los sistemas de riesgo limitado, el empresario que ponga a disposición de las personas trabajadoras sistemas de IA que impliquen riesgo mínimo, deberán realizar igualmente una evaluación del impacto.

---

<sup>25</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 110

<sup>26</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 90

<sup>27</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 90

<sup>28</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 90

<sup>29</sup>Reglamento (UE) nº 1169/2011 del Parlamento Europeo y del Consejo

### III. LA IA APLICADA A LA PREVENCIÓN DE RIESGOS LABORALES

La IA ofrece el potencial para desarrollos innovadores y emocionantes en el lugar de trabajo, pudiendo encontrarse aplicaciones muy variadas. Entre ellas, las aplicaciones IA en los procesos de trabajo van desde los cobots o equipos de protección individual inteligentes, hasta procesos algorítmicos en aplicaciones de recursos humanos como análisis de personas y gamificación.

Ante el gran abanico de oportunidades que ofrece, es también importante tener en cuenta los desafíos que plantea a nivel de seguridad y salud en el trabajo, su gestión y regulación<sup>30</sup>. De esta forma, teniendo como referencia el marco regulatorio propuesto en la Unión Europea, el presente trabajo tiene por objetivo identificar distintas prácticas o sistemas de Inteligencia Artificial aplicables al ámbito de la Prevención de Riesgos Laborales.

#### 1. Implicaciones de la IA en Prevención de Riesgos Laborales

El Reglamento de IA se ha desarrollado con objeto de poder ser aplicado, de forma transversal, en los distintos ámbitos en los que se puedan utilizar sistemas de IA, incluyendo el lugar de trabajo y en concreto, pudiendo enfocarse también al ámbito de la prevención de riesgos laborales.

Posteriormente analizaremos la variedad de formas en las que la IA puede ser utilizada dentro de la empresa con fines de mejorar la seguridad y salud en el trabajo. A pesar de ello, son varias las implicaciones y puntos sensibles con las que este tipo de sistemas se encuentran a la hora de ser utilizados por y para las personas trabajadoras, encajando así mismo con las restricciones ya marcadas por el propio Reglamento.

En primer lugar, siempre que hablamos de trabajos por cuenta ajena, debemos dar por hecho que se trata de una relación laboral en la que existe desigualdad de poder. Esta desigualdad se ve incluso incrementada cuando por determinadas características de la persona trabajadora, el empleador o empleadora puede llegar a discriminar a la persona trabajadora. Si combinamos esto con una tecnología que, normalmente, trabaja mediante aprendizaje a partir de la información de la que se le va alimentando y distintos patrones

---

<sup>30</sup>MACÍAS GARCÍA, María del Carmen. (2022) "La inteligencia artificial para el entorno laboral. Un enfoque en la predicción de accidentes". *e-Revista Internacional de la Protección Social*, 7 (1), 84-101.

que se le puedan ir enseñando, puede generar situaciones en las que la relación de poder y vulnerabilidad se vea incluso más marcada.

Asimismo, en prevención de riesgos laborales en ocasiones se requiere trabajar con datos de salud o información de carácter privado de las personas, por lo que es importante hacer un buen uso de este tipo de datos para, de nuevo, no generar daño en ninguna persona. Además de los daños desde el punto de vista de la salud, es evidente que los sistemas IA, dependiendo de la forma en la que se presenten, podrían igualmente suponer para los trabajadores riesgos más clásicos como son los golpes, choques o atrapamientos.

Por todo ello, la IA puede ser utilizada como instrumento para la mejora de la seguridad y salud de los trabajadores, pero, a pesar de ello, se deben tener en consideración los riesgos que su uso pudiera tener. Según indica la EU-OSHA, no es la tecnología como tal la que presenta los riesgos o beneficios para la seguridad y salud en el trabajo, sino la implementación que de ella se haga en la empresa<sup>31</sup>. Siendo esto así, El Reglamento de IA se debe interconectar con la normativa de seguridad y salud para hacerla segura para los trabajadores, que son, en realidad, los usuarios últimos de dichos dispositivos<sup>32</sup>.

## **2. Prácticas de inteligencia artificial prohibidas**

En primer lugar, por considerarse como la máxima categoría de riesgo, el Reglamento IA presenta una serie de prácticas sobre las que existe un total veto a su introducción en el mercado, puesta en servicio o utilización<sup>33</sup>. Comenzaremos analizando las características establecidas por el Reglamento para determinar qué sistemas de IA son inadmisibles y así, poder analizar a nivel de Prevención de Riesgos Laborales cuáles podrían quedar clasificados dentro de esta categoría.

En primer lugar, los sistemas de IA que puedan “*trascender la conciencia de una persona*” o que “*integren técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un grupo de personas mermando de manera apreciable su capacidad para adoptar una*

---

<sup>31</sup> LLORENS ESPADA, Julen. Límites al uso de la Inteligencia Artificial en el ámbito de la Salud Laboral, LA LEY Soluciones Legales, Madrid, 2023. Pag. 55

<sup>32</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 81

<sup>33</sup> LLORENS ESPADA, Julen (2023). Op. Cit. pag 30.

*decisión informada y causando así que la persona tome una decisión que de otro modo no habría tomado”.*

Aunque actualmente no son muchas los sistemas de IA aplicados al trabajo que pudieran encajar dentro de esta categoría son múltiples los usos que se le podría llegar a dar, a pesar de que algunos, pueden llegar incluso a ser sacados de la “fantasía” según indican Veale y Zuiderveen Borgesius. Estos autores, como ejemplo de una de las escenas sacadas de la serie “Black mirror” y que pudieran llegar a encajar en este percepto del anexo, mencionan unos sonidos inaudibles que se reproducen en las cabinas de los camiones para obligarlos, sin ser ellos conscientes, a conducir más tiempo del saludable y seguro. Para ello, se utiliza un sistema de IA que encuentra una frecuencia (para el sonido) mediante la cual consigue maximizar este efecto entre los conductores<sup>34</sup>. Esta práctica, además de trascender la conciencia de las personas e integran técnicas deliberadamente manipuladoras, generarían igualmente un perjuicio en la seguridad y salud de la persona, otro de los requisitos que posteriormente veremos.

Acercándonos algo más a la actual aplicabilidad que se le da a la IA en el trabajo, podría ser de aplicación en supuestos como el uso de la realidad virtual con fines de evitar accidentes en la empresa. La realidad virtual, se define como el entorno digital y tridimensional generado por ordenador, u otros sistemas informáticos, en el que una persona se siente inmersa en un espacio aparentemente real con cuyos elementos puede interactuar en mayor o menor medida<sup>35</sup>.

Esta, aplicada con fines de prevención de riesgos laborales, permite reproducir situaciones reales, en las que el usuario tiene libertad de acción y puede vivir, en primera persona, las consecuencias de sufrir un accidente laboral cuando no se adopten las medidas preventivas adecuadas. De esta forma, la simulación de situaciones permite a la persona vivir la experiencia de forma más intensa y con un importante impacto emocional de sensibilización<sup>36</sup>.

Este tipo de simulaciones, tienen la capacidad de hacer creer al usuario que realmente está viviendo el escenario que se le está proyectando. Siendo esto así, cuando es utilizada

---

<sup>34</sup> VEALE, Michael y ZUIDERVEEN BORGESIOUS, Frederik. “Demystifying the Draft EU Artificial Intelligence Act”, en *Computer Law Review International*, núm 22 (4), 2021

<sup>35</sup> FEMEVAL, Guía de Realidad Virtual y Realidad Aumentada, disponible en [https://www.femeval.es/dam/jcr:57a1b2aa-982b-40bd-b0f0-3b3d45bc162b/GUIA\\_RV\\_RA\\_link.pdf](https://www.femeval.es/dam/jcr:57a1b2aa-982b-40bd-b0f0-3b3d45bc162b/GUIA_RV_RA_link.pdf)

<sup>36</sup> GALINDO GARCÍA, Javier. ¿Sirve la realidad virtual para prevenir riesgos laborales? Disponible en <https://www.asepeyo.es/blog/seguridad-laboral/realidad-virtual-para-prevenir-riesgos-laborales/>

de forma correcta, simulando situaciones reales se mejora el aprendizaje y se fomenta adquirir buenos hábitos de seguridad. De forma contraria, en algunos supuestos dicha inmersión genera en la persona sensación de vulnerabilidad y falta de control sobre la situación, de forma que cada consecuencia tiene un impacto importante sobre la persona.

Ahora bien, a pesar de que mediante estas técnicas se podría llegar a lograr el cambio de comportamiento en las personas trabajadoras, debemos tener en cuenta que no se trata únicamente de alterar el comportamiento de las personas, sino de hacerlo de forma que dicha alteración del comportamiento pudiera suponer un perjuicio significativo. De esta forma, se sitúa como elemento central el perjuicio o daño<sup>37</sup> y se establece que no es necesario que el proveedor o el implementador tengan la intención de generar dicho perjuicio, siempre que este se derive de las prácticas de manipulación o explotación permitidas por el sistema (Considerando 5). Del mismo modo, el perjuicio generado debe ser “significativo”, dejando de lado aquellas situaciones en las que el daño no alcance la relevancia exigida, a pesar de que, sobre este concepto, el Reglamento no define o clarifica<sup>38</sup>.

Aunque el Reglamento de Inteligencia Artificial está planteado con el objetivo de poder ser implementado en variedad de áreas, la consecuencia de generar un perjuicio significativo puede entenderse como un punto contradictorio en si mismo aplicado a la prevención de riesgos laborales. Es decir, el objetivo principal de la prevención de riesgos laborales debe ser el de eliminar o reducir el riesgo de sufrir un accidente o enfermedad profesional, lo que significaría evitar cualquier perjuicio en la persona trabajadora. De esta forma, teniendo en cuenta que el daño y la manipulación deben ser intencionales, en la práctica, muy pocas herramientas entrarán dentro de esta categoría a nivel de empresa<sup>39</sup>.

A pesar de ello, en la actualidad se desarrollan nuevas formas de supervisión y gestión de personal a las hasta el momento, las personas trabajadoras no se han tenido que enfrentar. Como posteriormente analizaremos, los sistemas de IA diseñados para la gestión de personal en las empresas, quedan en principio categorizados como sistemas de alto riesgo. A pesar de ello, son dos los elementos con los que se debería tener especial cuidado a la hora de poner en uso este tipo de sistemas de control.

---

<sup>37</sup> LLORENS ESPADA, Julen (2023). Op Cit. pag. 31

<sup>38</sup> LLORENS ESPADA, Julen (2023). Op Cit. pag. 31

<sup>39</sup> AISLINN, K. “The AI Act and algorithmic management”, disponible en <https://cllpi.law.illinois.edu/content/dispatches/2021/Dispatch-No.-39.pdf>

En primer lugar, la sensación de estar siendo observado genera en la persona trabajadora una presión añadida a la hora de realizar el trabajo, ya que se busca hacerlo lo mejor posible mientras se está siendo supervisado. Esto significa que, dependiendo del tipo de medidas de control que se quieran implementar en la empresa (movimientos, constantes vitales, indicadores de estrés y fatiga o incluso expresiones micro-faciales, tono de voz y análisis de sentimientos), pueden generar que la persona trabajadora cambie su comportamiento y hábitos de trabajo con el fin de satisfacer expectativas.

Asimismo, la sensación de constante control, puede suponer invasión de la privacidad, provocando una fuente de ansiedad y estrés. Ambas consecuencias podrían llegar a considerarse alteraciones psicológicas del comportamiento, suponiendo un perjuicio, de carácter psicológico, en la persona trabajadora<sup>40</sup>.

Por otro lado, estarán prohibidos aquellos sistemas que pueden tener la capacidad de alterar el comportamiento mediante componentes subliminales imperceptibles para el ser humano o, en algunos casos, aprovechando la vulnerabilidad de una persona o un grupo específico de personas. El Reglamento hace referencia en su artículo 5 apartado 1 b, a las características conocidas o predichas de los rasgos de personalidad o la situación social o económica de esa persona o grupo, la edad y la capacidad física o mental.

Dentro del marco de la PRL, podrían encajar los trabajadores a los que la LPRL hace referencia, en su artículo 25, a las personas trabajadoras especialmente sensibles a los riesgos laborales. Se trata de personas trabajadoras que, como consecuencia de la interacción entre sus características personales, ya sea situación reconocida de discapacidad física, psíquica o sensorial y el trabajo que realizan, puedan ser especialmente sensibles a los riesgos con este relacionados. Asimismo, incluimos en este grupo a otros colectivos, que, por sus características, requieren de mayor protección por parte de la organización, como pueden ser las trabajadoras embarazadas o en periodo de lactancia, menores de edad y personal con relación laboral temporal.

En segundo lugar, serán también inadmisibles los sistemas de categorización biométrica que clasifiquen a las personas físicas con arreglo a atributos o características sensibles o protegidos, con exclusión de los dirigidos a fines terapéuticos (Considerando

---

<sup>40</sup> EU-OSHA, “Artificial intelligence for worker management: implications for occupational safety and health – Executive Summary” Disponible en <https://osha.europa.eu/es/publications/summary-artificial-intelligence-worker-management-implications-occupational-safety-and-health>

16 bis). Por lo tanto, no serán lícitas las categorizaciones de trabajadores en función de su información biométrica si estos datos se encuentran entre los que el Reglamento IA considera como sensibles o protegidos<sup>41</sup>.

De esta forma, no serán lícitas aquellas categorizaciones que provengan de datos como; *“el género y la identidad de género, la raza, el origen étnico. La condición de migrante o ciudadanía, la orientación política, la orientación sexual, la discapacidad o cualquier otro motivo por el que la discriminación esté prohibida”*. Todo ello atendiendo a la prohibición de discriminación establecida en el artículo 21 de la Carta de los Derechos Fundamentales (Considerando 16 bis). Se incluyen del mismo modo los datos especialmente sensibles del Reglamento General de Protección de datos, como pueden ser los datos genéticos o de salud<sup>42</sup>. La vía excepcional del tratamiento con objetivos terapéuticos no podrá tener cabida dentro del marco de la prevención de riesgos laborales, por estar dirigido a la prevención y no al tratamiento de enfermedades<sup>43</sup>.

Estarán igualmente prohibidas las prácticas de clasificación social de personas, que del mismo modo pudieran tener resultados discriminatorios, así como la exclusión de determinados grupos. Dichas clasificaciones se realizarán a través de datos y sucesos temporales relacionados con el comportamiento de las personas a las que se esté analizando, pudiendo provocar un trato desfavorable para estas o para colectivos enteros determinados, a pesar de no guardar relación directa con la situación de análisis (Considerando 5 bis).

En este sentido, como más adelante veremos, se trata de perseguir que los sistemas de IA se alimenten de información que elimine sesgos discriminatorios y que en dicha clasificación que aquí se menciona, se persiga un trato desfavorable para determinados grupos. Es decir, los sistemas IA prohibidos, lo estarán cuando en la clasificación social de personas subyazca una discriminación o trato desfavorable, pero no en aquellos casos en los que la categorización, sea generada con fines de procurar la seguridad y salud de la persona trabajadora.

En tercer lugar, *“los sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir*

---

<sup>41</sup> LLORENS ESPADA, Julen (2023). Op. Cit. pag.31

<sup>42</sup> LLORENS ESPADA, Julen (2023). Op. Cit. pag.30

<sup>43</sup> LLORENS ESPADA, Julen (2023). Op. Cit. pag.32

*de internet o de imágenes de circuito cerrado de televisión*”<sup>44</sup>. De este modo quedarán prohibidas las grabaciones de videovigilancia en la empresa que acometan reconocimiento facial no selectivo de las imágenes faciales de los trabajadores para la alimentación de base de datos. Se considera que este tipo de control agrava el sentimiento de vigilancia masiva y puede dar lugar a graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad, por lo que su práctica debe quedar prohibida<sup>45</sup>.

En cuarto lugar, se prohibirán también los sistemas de IA con *capacidad de inferir las emociones, los cuales pueden generar riesgos de abuso en diversos contextos, en los que expresamente incluye los lugares de trabajo* (Considerando 26 quater). Como ejemplo de ello, podrían ser los supuestos de interacción humano-robot. Se ha demostrado que esta relación va mucho más allá de coordinación de contenido o actividades y parte de su éxito está directamente relacionado con la capacidad del robot para percibir o inferir el estado emocional de la persona<sup>46</sup>.

La ISO 10218-1 de 2011, define robot industrial como “un manipulador controlado automáticamente, reprogramable y multifuncional, programable en tres o más ejes, que puede ser fijo o móvil y se utiliza en aplicaciones industriales automatizadas”. Desde el punto de vista de la prevención de riesgos laborales, es que los robots ayuden en tareas que para las personas pueden resultar insalubres, inseguras, tediosas o penosas, evitando su exposición a condiciones peligrosas y reduciendo los riesgos tanto físicos, como ergonómicos y psicosociales<sup>47</sup>.

A diferencia de estos, que pueden mantener mayor similitud con una simple máquina, encontramos también la figura de “cobot” o robot colaborativo. Estos son definidos por la Agencia Europea de Seguridad y Salud en el Trabajo como “robots concebidos para la interacción directa con un humano dentro de un espacio de trabajo

---

<sup>44</sup> Art 5.1 d Reglamento Inteligencia Artificial

<sup>45</sup> LLORENS ESPADA, Julen (2023). Op. Cit. pag.32

<sup>46</sup> MARTÍNEZ, Fredy, HERNÁNDEZ, César y GIRAL, Diego “Sistema integrado de reconocimiento de emociones para interacción hombre-máquina”. *Información tecnológica*, 34(1), 117-128.

<sup>47</sup> MIRA PÉREZ, Paula. “Prevención de Riesgos Laborales en la Industria 4.0” Universidad de Valladolid (2020)

colaborativo determinado y con un diseño seguro, adaptable y de fácil manejo, a menudo con rasgos humanos, como dos brazos y expresiones faciales”<sup>48</sup>.

Este último tipo de robot encaja más en el descrito al principio, es decir, que integrando otro tipo de capacidades cognitivas, es capaz de, aunque sea de forma artificial, crear una conexión “emocional” con la persona que se trabaja. A pesar de que en algunos estudios se destaca el lado positivo de la integración de este tipo de capacidades en los robots, en determinados contextos como el laboral, puede suponer un problema, como indica en el Reglamento. Por ello, no quedará prohibido el uso de robots o cobots en el entorno laboral, destinados a liberar a las personas de las tareas más precarias, ni tan siquiera aquellos que integren habilidades cognitivas. A pesar de ello, sí quedarán prohibidos los que mediante inferencia de emociones puedan aprovechar situaciones de vulnerabilidad en las personas trabajadoras.

### **3. Prácticas de inteligencia artificial de alto riesgo**

Serán considerados sistemas de IA de “alto riesgo” aquellos que *“tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión”*. A la hora de determinar si se trata de un sistema que encaje dentro de alto riesgo, se deberá revisar la magnitud de las consecuencias respecto a los derechos fundamentales de la Unión, entre los que se incluyen: derecho a la dignidad humana, respeto a la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión (...) (Considerando 28 bis).

En primer lugar, se debe tener en cuenta que los sistemas de alto riesgo se articulan mediante dos fórmulas acumuladas (art. 6 Reglamento IA):

a) Sistemas destinados a ser utilizados como componentes de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión, o que el sistema en sí mismo sea uno de dichos productos, establecidos en el Anexo II de este mismo Reglamento.

---

<sup>48</sup> Tesaurus de la EU-OSHA. Disponible en: <https://osha.europa.eu/es/tools-and-resources/eu-osha-thesaurus/term/70027i>

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

En relación a la lista de productos detallados en el Anexo II, desde el punto de vista de la PRL, nos interesan especialmente, la Directiva de máquinas<sup>49</sup>, el Reglamento de equipos de protección individual<sup>50</sup> y el Reglamento sobre los productos sanitarios<sup>51</sup>. Del mismo modo, se relacionan nominativamente una serie de sistemas de IA cuyos riesgos ya se han materializado o existe un elevado consenso en la probabilidad de que se materialicen en un futuro próximo. De esta forma, el anexo III establece una serie de áreas en las cuales, cualquier implementación de sistema IA implicará su categorización como de alto riesgo. Como anteriormente hemos mencionado, nos interesarán concretamente el punto 1: *identificación biométrica y categorización de personas físicas*, así como el punto 4: *empleo, gestión de los trabajadores y acceso al autoempleo*.

En relación al primer punto, se incluirán todos aquellos sistemas biométricos y basados en la biometría, destinados a utilizarse en la identificación biométrica de las personas físicas o para extraer conclusiones sobre las características personales de las personas físicas a partir de datos biométricos o basados en la biometría, incluidos los sistemas de reconocimiento de emociones.

En este punto, se debe tener en cuenta que, los sistemas de categorización biométrica se definen como un sistema de IA destinado a asignar a las personas físicas a categorías específicas, como sexo, edad, (...), rasgos personales, origen étnico u orientación sexual o política, sobre la base de sus datos biométricos. Asimismo, los sistemas de

---

<sup>49</sup> Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24) [derogada por el Reglamento relativo a las máquinas]

<sup>50</sup> 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)

<sup>51</sup> Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1)

reconocimiento de emociones son sistemas de IA destinados a identificar o inferir emociones o intenciones de personas físicas a partir de sus datos biométricos<sup>52</sup>.

Es importante clarificar la distinción entre la identificación de emociones que se mencionaba en el apartado de prácticas prohibidas, y la que ahora encontramos. En este sentido, el punto 5.1 del Reglamento y, por lo tanto, prácticas clasificadas como prohibidas, serán aquellas dirigidas a “*inferir las emociones*” de las personas trabajadoras, mientras que serán de alto riesgo las destinadas a “*extraer conclusiones*” teniendo como base la detección de emociones<sup>53</sup>.

Por otro lado, en relación al segundo punto, el cual se refiere a los sistemas de IA en materia de empleo, gestión de los trabajadores y acceso al autoempleo, se diferencian dos categorías. En primer lugar, “*sistemas de IA destinados a utilizarse para la contratación o selección de personas físicas, especialmente para anunciar puestos vacantes, clasificar y filtrar solicitudes o evaluar a candidatos en el transcurso de entrevistas o pruebas*” y en segundo lugar, “*Sistemas de IA destinados a utilizarse para tomar decisiones o influir sustancialmente en ellas que afecten a la iniciación, promoción y resolución de las 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 las personas en el marco de dichas relaciones*”<sup>54</sup>.

Juntando todos estos requisitos legales, encontramos la posibilidad de prevenir accidentes laborales a través de la detección del comportamiento de las personas. En el contexto de la empresa y, atendiendo tanto a la LPRL como al marco legal existente en Europa, el empresario debe garantizar la seguridad y salud de las personas, eliminando o reduciendo los riesgos. Esto implica que debe conocer los riesgos a los que los trabajadores están expuestos y proponer medidas para evitar que estos sufran un accidente de trabajo o enfermedad profesional. Asimismo, las personas trabajadoras tienen la responsabilidad de trabajar de manera segura y protegerse a sí mismo y a otros trabajadores.

---

<sup>52</sup> COTINO HUESO, Lorenzo “Sistemas de inteligencia artificial con reconocimiento fácil y datos biométricos. Mejor regular bien que prohibir mal” en *El Cronista del Estado y Democrático de Derecho*, núm. 100, 2022

<sup>53</sup> LLORENS ESPADA, Julen (2023). Op. Cit pag 37.

<sup>54</sup> Anexo III Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2 del Reglamento IA

A pesar de las medidas que se puedan aplicar desde el punto de vista técnico, el factor humano está detrás del 80% de los accidentes laborales, por lo que también es importante comprender y atender este aspecto<sup>55</sup>. En este sentido, existen diversas características cognitivas o de personalidad, que predisponen a las personas, en mayor o menor medida, hacia determinados comportamientos y por lo tanto, haciéndolos más o menos propensos a sufrir accidentes de trabajo.

En este sentido, hay autores que defienden que la IA es capaz de estimar la predisposición al accidente en determinados contextos, con base en tendencias de comportamientos naturales<sup>56</sup>. De esta forma, se defiende igualmente la aplicabilidad de esta información para la obtención de información aparentemente objetiva sobre las personas incluso antes de contratarlas. Esto se conseguiría mediante aplicaciones de IA que recopilen información sobre las actividades de los trabajadores y de los aspirantes a un puesto de trabajo, vigilando sus movimientos físicos y sentimientos<sup>57</sup>.

Es cierto que, en este supuesto, se habla de sentimientos, mientras que el Reglamento se refiere a emociones, y aunque su distinción y categorización entra dentro del campo de la psicología, es importante tenerlo en cuenta a la hora de recopilar información. Siendo esto así, a la hora de diferenciarlas, podríamos tener como referencia que, la emoción y reacciones emocionales están alineadas con el cuerpo, mientras que los sentimientos con la mente. De esta forma, la emoción se presenta como una reacción relacionada con la conciencia inmediata, es breve, pero intensa, mientras que el sentimiento, dura más tiempo y en principio, es menos intenso, además de estar más relacionado con el aspecto cognitivo<sup>58</sup>. En algunas ocasiones, se dice también que los sentimientos son la expresión a nivel mental de las emociones<sup>59</sup>.

---

<sup>55</sup> Sociedad Española de Salud y Seguridad en el Trabajo (2021) "El Uso de Sistemas de Inteligencia Artificial Para Reducir la Siniestralidad en el Trabajo". Disponible en <https://www.sesst.org/e-prevenir-a-predecirel-uso-de-sistemas-de-inteligencia-artificial-para-reducir-lasiniestralidad-en-el-trabajo/>

<sup>56</sup> MOORE, Phoebe. "Inteligencia artificial en el entorno laboral. Desafíos para los trabajadores". Universidad de Leicester, 2020. <https://www.bbvaopenmind.com/articulos/inteligencia-artificial-en-entorno-laboral-desafios-para-trabajadores/>

<sup>57</sup> VALLEJO NOGUERA, Franco Fernando, RUBIO ENDARA, Omar Washington y TELLO MOREIRA, José Antonio. "Implementar el Uso de la Inteligencia Artificial para Detectar el Comportamiento del Trabajador en la Prevención de Accidentes Laborales en la Empresa". *Dominio de las Ciencias*, 8(1), 21.

<sup>58</sup> Poncela, A. M. F. (2012). Antropología de las emociones y teoría de los sentimientos. *Versión. Estudios de Comunicación y Política*, (26), 315-339.

<sup>59</sup> DAMASIO, Antonio (2006) "El error de Descartes. La emoción, la razón y el cerebro humano". Barcelona

Siguiendo con el Reglamento, se hace referencia a aquellas áreas o situaciones en las que los sistemas de IA *“pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, ciertos grupos de edad, personas con discapacidad o personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, la promoción o la retención de personas en relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden afectar a sus derechos a la protección de los datos personales y a la privacidad”* (Considerando 36).

A esto se le añaden que, en el marco normativo español, la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, en la que se establece que, nadie podrá ser discriminado por razón de nacimiento, origen racial o étnico, sexo, religión, convicción u opinión, edad, discapacidad, orientación o identidad sexual, expresión de género, enfermedad o condición de salud, estado serológico y/o predisposición genética a sufrir patologías y trastornos, lengua, situación socioeconómica, o cualquier otra condición o circunstancia personal o social<sup>60</sup>.

Del mismo modo, y a pesar de que actualmente esta misma ley hace referencia únicamente a la administración pública, se debe favorecer la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas. De nuevo, se pretende abordar el potencial impacto discriminatorio que los sistemas de IA pudieran llegar a tener en las personas que encajen en alguno de esos colectivos.

De nuevo, volvemos a la idea de que el Reglamento persigue proteger a determinados colectivos de los históricos patrones de discriminación. A pesar de ello, en algunos supuestos a los que tanto el Reglamento como la Ley hacen referencia, como pueden ser, personas con discapacidad, religión enfermedad o condición de salud o el estado serológico y/o predisposición genética a sufrir patologías y trastornos, son características que, en determinados contextos de trabajo, la persona pueda ser especialmente sensible a los riesgos.

Siendo esto así, dentro de la relación laboral encontraremos a un trabajador especialmente sensible y, por lo tanto, la obligación de adaptar el puesto de forma que la

---

<sup>60</sup> Artículo 2, Ley 15/2022, de 12 de julio, Integral para la igualdad de trato y la no discriminación.

persona pueda seguir desarrollando su trabajo sin sufrir daño, además de la prohibición de ser discriminado o recibir trato desfavorable por dicha circunstancia. Este tipo de situaciones tendrán que hacerse de forma justificada y sin que en ellas haya un fin discriminatorio, ya que, el artículo 9.2 de la Ley anteriormente mencionada, hace referencia a que “se entenderán discriminatorios (...) condiciones de trabajo que produzcan situaciones de discriminación indirecta por razón de las causas previstas en esta ley”.

Teniendo como referencia lo establecido por el Reglamento en relación a sistemas de IA de alto riesgo, a continuación, analizaremos como algunas de las herramientas ya existentes en el mercado podrían llegar a encajar en dicha clasificación. Siendo esto así, nos centraremos en analizar, los Equipos de Protección Individual Inteligentes, los Software de gestión preventiva y el trabajo en plataformas digitales.

### *3.1.EPIs inteligentes*

En primer lugar, el Comité Europeo de Normalización (CEN) define los EPI inteligentes como “*equipos de protección individual que (...) muestran una respuesta finalista y práctica, ya sea a los cambios del entorno/ medio o a una señal/ indicación externa*”<sup>61</sup>. Asimismo, la OSHA se refiere a ellos como aquellos que combinan el EPI tradicional, como puede ser una prenda de protección, con materiales mejorados o componentes electrónicos, como pueden ser sensores o detectores, dirigidos a aumentar el nivel de protección.

Como anteriormente se ha mencionado, quedan regulados en el Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016<sup>62</sup>, relativo a los equipos de protección individual. Siendo esto así, serán considerados sistemas de IA de alto riesgo cuando por las características, encajen en el Anexo II y requiera de la evaluación de un tercero. Este requisito será necesario en supuestos como el de EPIs contra sustancias peligrosas, radiaciones, descargas eléctricas, etc.

---

<sup>61</sup> Definición 10.1 en el documento CEN/TC 162/WI 439, de julio de 2019

<sup>62</sup> Además de esto, la CEN ha publicado una guía sobre textiles inteligentes: CEN/TR 16298:2911: Textiles y productos textiles. Textiles inteligentes. Definiciones, categorización, aplicaciones y necesidades relativas a la normalización.

Para su clasificación, la OSHA ha propuesto la categorización de estos atendiendo a su composición (si cuentan o no con elementos electrónicos) y a la capacidad para recoger datos (no recoge datos, únicamente recoge datos no personales y con recogida de datos personales) que tenga el equipo<sup>63</sup>. De esta forma, son diversas las formas en las que podemos encontrar este tipo de EPIs, desde los más simples que sin incorporar elementos electrónicos cuentan con materiales mejorados, hasta aquellos que cuentan con elementos electrónicos integrados.

En referencia a estos últimos, entre aquellos que aun contando con elementos electrónicos no recogen datos personales, existen prendas de “visibilidad inteligente” que incorporan iluminación, mientras que, también encontramos EPIs que, sin necesidad de recopilar datos personales, recogen información sobre el uso que se le da al equipo o con capacidad de recoger datos del entorno en el que se utilizan.

En último lugar, encontramos lo EPIs que recogen datos de carácter personal. Este tipo de equipos generan nuevos peligros relacionados con el tratamiento masivo de datos, de forma deberán cumplir con el Reglamento General de Protección de datos y realizar evaluaciones de impacto en materia de datos personales. En cualquier caso, siempre que estos equipos sean categorizados dentro de los sistemas de IA de alto riesgo, deberán igualmente realizar la correspondiente evaluación de conformidad.

### *3.2. Software de gestión preventiva (AIWM)*

En segundo lugar, los software de gestión preventiva son sistema de gestión de trabajadores que recopila datos, a menudo en tiempo real, del espacio de trabajo, los trabajadores y el trabajo que realizan, para posteriormente ser introducidos en un sistema basado en IA que toma decisiones automatizadas o semiautomatizadas, o proporciona información para las personas que deben tomar decisiones, sobre cuestiones relacionadas con la gestión de los trabajadores<sup>64</sup>. La Agencia Europea de Seguridad y Salud en el

---

<sup>63</sup> EU-OSHA, “Equipos de protección individual inteligentes: protección inteligente de cara al futuro” Disponible en: <https://osha.europa.eu/es/publications/smart-personal-protective-equipment-intelligent-protection-future>

<sup>64</sup> EU-OSHA, “Artificial intelligence for worker management: implications for occupational safety and health – Executive Summary” Disponible en <https://osha.europa.eu/es/publications/summary-artificial-intelligence-worker-management-implications-occupational-safety-and-health>

Trabajo se refiere a ellos como AIWM, lo que traduciendo las siglas en inglés significaría “inteligencia artificial para la gestión de trabajadores”.

Debido al propósito para el que está diseñado, encajaría en el cuarto punto del Anexo III anteriormente mencionado (empleo, gestión de trabajadores y acceso al autoempleo), en cuanto se utiliza para la gestión de trabajadores y “para la asignación de tareas y el seguimiento”.

Este tipo de software suele ir acompañado de otros dispositivos electrónicos que ayudan a recopilar información tanto de la persona como de su entorno, de esta forma, el sistema hace una recopilación de datos que, en conjunto, permite determinar la repercusión que el entorno pueda tener en el trabajador, así como tomar decisiones al respecto y evitar accidentes de trabajo<sup>65</sup>.

Del mismo modo, la EU-OSHA destaca como beneficios, las alertas tempranas y advertencias sobre riesgos para la seguridad y salud de los trabajadores, el análisis de la eficiencia de diferentes soluciones y la propuesta de intervención para mejorar la seguridad y salud en el trabajo<sup>66</sup>.

Por lo contrario, a pesar de los múltiples usos beneficiosos que se le puede dar para proteger a las personas trabajadoras de condiciones o actos inseguros, la realidad es que, los datos recogidos, se utilizan también para la toma de decisiones para la mejora de la eficiencia productiva. Este tipo de uso de la información vuelve a generar riesgo de que determinados colectivos de trabajadores y trabajadoras puedan llegar a ser discriminados o recibir un trato desigual debido a los índices obtenidos por la IA.

Así pues, este tipo de sistemas se podrían implementar en la empresa con el objetivo de predecir sucesos peligrosos, disminuir la siniestralidad y para la mejora de la seguridad y salud de las personas trabajadoras. Por lo contrario, no deberían utilizarse para la búsqueda de eficiencia productiva, evaluar el rendimiento del trabajador o tomar decisiones discriminatorias.

De esta forma, volveríamos de nuevo a la idea anteriormente mencionada. Siendo esto así, cabe diferenciar las situaciones en las que, por determinadas características de la

---

<sup>65</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 98

<sup>66</sup> EU-OSHA, “Artificial intelligence for worker management: implications for occupational safety and health – Executive Summary” Disponible en <https://osha.europa.eu/es/publications/summary-artificial-intelligence-worker-management-implications-occupational-safety-and-health>

persona trabajadora, exista especial sensibilidad a determinados riesgos y, por lo tanto, la necesidad de adaptación del trabajo en ese contexto. En este tipo de situaciones, los sistemas de gestión de IA pueden ser muy útiles y más eficaces a la hora de organizar el trabajo y al personal.

A modo de ejemplo, tanto el Reglamento IA como la Ley 15/2022 mencionan la religión como característica por la que una persona no puede ser discriminada o recibir un trato desfavorable. Ahora bien, como ejemplo, en la religión musulmana durante un periodo del año se celebra el Ramadán, lo que implica que, entre otras, los musulmanes se abstienen de comer y beber. A nivel fisiológico, esa falta de alimentación o hidratación puede generar problemas cuando se trabaja en determinados contextos que requieren de mayor esfuerzo físico o igualmente en verano, cuando se trabaja en altas temperaturas.

En dicha situación, tanto el software como otros elementos, como pudiera ser un reloj inteligente, podrían ayudar a detectar situaciones en la que la persona trabajadora está exponiéndose a un mayor riesgo de sufrir un daño, por falta de hidratación o cualquier otra característica. En este sentido, aunque la organización del trabajo se realizase mediante algoritmos que tuviesen en cuenta distintos filtros, entre los que se incluiría la religión, resultaría imprescindible la intervención humana a la hora de tomar la decisión final, de forma que no exista discriminación en tal decisión. Las decisiones tomadas a través de un sistema IA harían uso de filtros en el algoritmo, entre los que se incluiría el ámbito religioso.

### *3.3. Trabajo en plataformas digitales*

Por último, nos referimos al trabajo en plataformas digitales a todo trabajo remunerado proporcionado a través de, o mediado por, una plataforma en línea. De esta forma, mediante gestión algorítmica, se asignan tareas y se monitorea y evalúa el comportamiento y desempeño de las personas trabajadoras<sup>67</sup>. El ejemplo más simbólico de este tipo de relaciones laborales es el de reparto de domicilio (Riders).

En el caso de este tipo de trabajos, se desarrollan mediante una aplicación conectada a una plataforma que va indicando donde cada persona trabajadora debe recoger las

---

<sup>67</sup> EU-OSHA, “Trabajo en plataformas digitales: consecuencias para la salud y seguridad en el trabajo” Disponible en: <https://osha.europa.eu/es/publications/digital-platform-work-implications-occupational-safety-and-health>

mercancías y realizar las entregas<sup>68</sup>. Siendo esto así, la propia plataforma, utiliza algoritmos para la asignación de tareas y vincula automáticamente a los trabajadores con los clientes, condicionando tal decisión en base a indicadores como las puntuaciones, reseñas de clientes, índices de cancelación o aceptación de trabajo y los perfiles de los trabajadores<sup>69</sup>. De esta forma, este tipo de sistemas que aplican IA entrarían dentro de la categoría de alto riesgo en tanto que se utilizan para “*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 las personas en el marco de dichas relaciones*”.

A pesar de que, en principio, todas las personas trabajando con estas plataformas son evaluadas de la misma manera, según indica la Organización Internacional del Trabajo, el proceso de asignación algorítmica también puede tener en cuenta los planes de suscripción y los paquetes opcionales adquiridos, pudiendo generar exclusión de las personas procedentes de países en desarrollo y a los que tienen ingresos más bajos. De esta forma, independientemente de los motivos adicionales que pueda haber para la asignación de tareas, la organización y repartición de tareas llevada a cabo por este tipo de plataformas, cabría clasificarse como de alto riesgo, debiendo cumplir todos los requisitos y obligaciones que esto implica.

### *3.4. Requisitos de los sistemas de alto riesgo y obligaciones*

Una vez delimitados los sistemas de alto riesgo, el Capítulo II del Título III, regula los requisitos que deben reunir estos sistemas para poder implantarse estando sujetos a una serie de restricciones y mecanismos de control *ex ante* y *ex post* que garanticen la aplicación efectiva del Reglamento<sup>70</sup>, y asegurando el nivel de protección esperado, en relación a la salud, la seguridad y los derechos fundamentales. Para la comprobación del cumplimiento de los requisitos de estos sistemas de alto riesgo, será determinante la

---

<sup>68</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 101

<sup>69</sup> OIT, “Perspectivas Sociales y del Empleo en el Mundo. El papel de las plataformas digitales en la transformación del mundo del trabajo”. Disponible en: [https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms\\_771675.pdf](https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_771675.pdf)

<sup>70</sup> GAMERO CASADO, Eduardo (2021). Op. Cit. Pag.282

finalidad prevista del sistema, los usos indebidos razonablemente previsibles y el sistema de gestión durante todo el ciclo de vida del sistema de IA<sup>71</sup>.

En primer lugar, el artículo 9.1 del Reglamento IA establece la obligatoriedad de implantar, documentar y mantener un sistema de gestión de riesgos. Este sistema consistirá en un proceso iterativo a llevar a cabo durante todo el ciclo de vida del sistema IA de alto riesgo, debiendo revisarse y actualizarse de forma periódica (art 9.2 Reglamento IA).

El sistema de gestión constará de cuatro fases (art 9.2 Reglamento IA). Se iniciará con *“la identificación, la estimación y la evaluación de los riesgos conocidos y razonablemente previsibles que el sistema de IA de alto riesgo pueda plantear para la salud o la seguridad de las personas físicas, sus derechos fundamentales, incluida la igualdad de acceso y oportunidades, la democracia y el Estado de Derecho o el medio ambiente”*, continuado por *“la evaluación de los riesgos significativos emergentes descritos en la letra a) y detectados a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización”* y finalizará con *“la adopción de medidas apropiadas y específicas de gestión de riesgos diseñadas para abordar los riesgos detectados de conformidad con las letras a) y b) del presente apartado con arreglo a lo dispuesto en los apartados siguientes”*.

En este sentido, no se impone a los proveedores la obligación de eliminar el riesgo, sino que se identifique, reduzca y controle, proporcionando información. De esta forma, siempre que las medidas de gestión de riesgos sean suficientes y el sistema sea utilizado para la finalidad prevista (o en uso indebido razonablemente previsible), los riesgos residuales serán aceptables, siempre que estos sean comunicados<sup>72</sup>.

Se debe tener en cuenta que, los sistemas de IA de alto riesgo, debe cubrir no solo los riesgos específicos de seguridad de IA, sino la seguridad del producto final. De esta forma, el proveedor se verá igualmente obligado a realizar la evaluación desde la perspectiva preventiva de la seguridad y salud de los trabajadores.

---

<sup>71</sup> LLORENS ESPADA, Julen (2023). Op. Cit Pag.39

<sup>72</sup> PONCE, Aida. “The AI Regulation: Entering an AI Regulatory Winter? Why An Ad Hoc Directive on Ai in Employment Is Required” European Trade Union Institute (ETUI) Research Paper. Disponible en: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3873786](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873786)

La realización de la evaluación de conformidad es una de las obligaciones impuestas al proveedor antes de introducir el sistema de IA al mercado, debiendo hacerla bajo su propia responsabilidad. Mediante la realización de esta los proveedores demostrarán el cumplimiento de los requisitos obligatorios a los que a continuación haremos referencia.

Atendiendo al artículo 19 del Reglamento IA, cuando mediante la evaluación de conformidad se demuestre que los sistemas cumplen los requisitos establecidos en el capítulo 2 del Título Tercero los proveedores elaborarán una declaración UE de conformidad con arreglo al artículo 48 y colocarán el marcado CE de conformidad con arreglo al artículo 49.

Por otro lado, atendiendo al artículo 10 Reglamento IA, la calidad de los datos utilizados para la programación es uno de los grandes desafíos de los sistemas IA, ya que utilizar datos inadecuados puede implicar sesgos, por lo que estos datos deben cumplir con criterios de calidad concretos. Asimismo, atendiendo al artículo 64.4 del Estatuto de los Trabajadores, se deberá informar a los representantes de los trabajadores “de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afecten a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles”.

Del mismo modo, una de las exigencias más reiteradas por la doctrina jurídica en relación con los sistemas de IA, es la necesidad de garantizar su transparencia. De esta forma, los sistemas de IA deben ser diseñados de forma que los proveedores y usuarios entiendan razonablemente el funcionamiento del sistema<sup>73</sup>.

Por otro lado, los sistemas de IA de alto riesgo se deben diseñar y desarrollar de forma que puedan ser supervisados de manera efectiva por personas físicas, debiendo incluir también una herramienta de interfaz humano-máquina adecuada. El requisito de la intervención humana viene también establecido en el artículo 22 de RGPD, en el que se establece que los interesados tendrán derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos. Del mismo modo, el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos u

---

<sup>73</sup>GAMERO CASADO, Eduardo (2021). Op. Cit Pag. 282.

libertades y los intereses legítimos del interesado, como mínimo, el derecho a obtener intervención humana (Artículo 22 RGPD).

En último lugar, los sistemas de IA de alto riesgo deben ser diseñados y desarrollados con capacidades que permitan registrar automáticamente eventos (“archivo de registro”), mientras estén en funcionamiento. Siendo esto así, será obligación del proveedor, mientras el sistema esté bajo su control, conservar dichos archivos de registro, siendo estos necesarios para garantizar y demostrar el cumplimiento del Reglamento<sup>74</sup>.

De forma distinta, será más adelante obligación del implementador, es decir, el empleador o empleadora en el caso que nos aplica, llevar a cabo una evaluación del impacto en los derechos fundamentales. Esta evaluación deberá comprender, como mínimo, una descripción clara de la finalidad prevista, del ámbito geográfico y temporal previsto, categorías de personas físicas y grupos que puedan verse afectados, una verificación de que la utilización del sistema es conforme al Derecho de la Unión, el impacto razonablemente previsible en los derechos fundamentales, los riesgos de perjuicio específicos que puedan afectar a personas marginadas o grupos vulnerables, repercusiones negativas razonablemente previsibles del uso del sistema en el medioambiente, plan detallado de mitigación de perjuicios y sistema de gobernanza del implementador (Artículo 29 Reglamento IA).

#### **4. Sistemas de Inteligencia Artificial de riesgo limitado y mínimo**

Este tipo de sistemas son los destinados a interactuar con personas físicas y sistemas de reconocimiento de emociones o de categorización biométrica en cuanto al funcionamiento de los mismos o sistemas que generen manipulación de imágenes y sonidos y que puedan inducir erróneamente a una persona a pensar que son auténticos o verídicos.

Para este tipo de sistemas, el Reglamento únicamente establece la obligación de transparencia para los proveedores, debiendo garantizar que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA<sup>75</sup>. Asimismo,

---

<sup>74</sup> Artículos 12 y 16.1 Reglamento IA

<sup>75</sup> Artículo 52 Reglamento IA

se informará cuando el contenido visualizado haya sido generado de forma artificial, cuando pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos (ultrafalsificación).

A modo de ejemplo, cuando hay cualquier tipo de accidente, con consecuencias más o menos importantes o incluso un incidente, en el que no hay daño personal ni material, mostrar imágenes sobre el suceso o consecuencias a las personas trabajadoras ayuda a que comprendan mejor la situación. Asimismo, cuando en ese suceso se ha generado un daño, mostrar imágenes o videos suele generar un mayor impacto en las personas y, por lo tanto, un cambio más efectivo de actitud.

Siendo esto así, la ultrafalsificación o “deepfake” podría ser utilizado para recrear, ya sean escenarios reales o ficticios, de situaciones que podrían llegar en el contexto laboral en el que nos encontremos. De esta forma, las personas trabajadoras podrían visualizar de forma más sencilla las consecuencias que el no cumplimiento de las normas preventivas o la realización de un acto inseguro pudieran tener en su seguridad y salud. Este tipo de técnicas serían utilizadas siempre informando a las personas de que dichas imágenes o videos han sido elaboradas mediante IA, pero que el contenido mostrado efectivamente podría darse en la realidad.

Por último, los sistemas de IA de riesgo mínimo Los categorizados en este último bloque se consideran sistemas que no implican riesgo, por lo que únicamente tendrán que cumplir con el resto de legislación vigente, sin requisitos adicionales por parte del Reglamento. Por otro lado, se deja a elección del proveedor la posibilidad de aplicar, voluntariamente, otros requisitos, además de la adhesión a códigos de conducta<sup>76</sup>.

Actualmente, se considera que la mayoría de los sistemas IA utilizados en la UE pertenecen a esta categoría, asimismo, aquellos sistemas que no alcancen el impacto perjudicial significativo establecido para los sistemas de alto riesgo, encajarán en esta categoría. Siendo esto así, son variadas las formas en las que la Inteligencia Artificial se ha ido haciendo hueco para colaborar en la prevención de riesgos laborales de las empresas. Todas ellas, independientemente de que se ajusten en menor o mayor medida a los riesgos mencionados por el Reglamento IA, siguen teniendo igualmente la posibilidad de generar otros riesgos más clásicos entre los trabajadores, como pueden ser

---

<sup>76</sup> GOÑI SEIN, José Luis (2023). Op Cit. Pág. 89

choques, golpes o incluso a nivel psicosocial, como puede ser el estrés la ansiedad o la falta de autonomía.

#### IV. OBLIGACIONES DEL USUARIO O EMPLEADOR

En primer lugar, el Reglamento IA establece en su artículo 4 bis los principios generales aplicables a todos los sistemas de IA. El primero de ellos, la “*intervención y vigilancia humana*”, lo cual implicará que los sistemas IA se desarrollen y utilicen como una herramienta al servicio de las personas, respetando la dignidad humana y la autonomía personal, pudiendo ser controlada y vigilada adecuadamente por seres humanos. En segundo lugar, “*Solidez y seguridad técnica*”, de forma que todos los sistemas se desarrollarán y utilizarán de manera que se minimicen los daños imprevistos e inesperados, así como para ser sólidos en caso de problemas imprevistos y resistentes a los intentos de modificar su uso. En tercer lugar, “*Privacidad y gobernanza de datos*”, “*Transparencia*”, “*diversidad, no discriminación y equidad*” “*Bienestar social y medioambiental*”

Además de los principios generales y las obligaciones anteriormente mencionadas para los sistemas de alto riesgo, el empresario deberá cumplir con otras obligaciones con el fin de velar por la seguridad y salud en el trabajo. En primer lugar, es importante tener en cuenta que, lo que en un primer momento el Reglamento IA definía como “usuario” actualmente se refiere a “implementador”, en su artículo 3. De esta forma, atendiendo al artículo 3 del Reglamento IA, se considerará implementador a “*toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice in sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional*”. De esta forma, consideraremos como implementador a los empresarios que utilicen sistemas IA como medio de producción en la empresa<sup>77</sup>.

Por otro lado, como ya sabemos, el empleador es el último responsable de la seguridad y salud de los empleados y empleadas. Siendo esto así, la primera de las obligaciones que se le atribuye al empresario en esta materia es la de integrar en el ámbito laboral productos que sean seguros.

---

<sup>77</sup>RODRIGUEZ SANZ DE GALDEANO, Beatriz (2023). Op Cit. Pág. 61

De esta forma, en lo que se refiere a equipos de trabajo, la LPRL establece en su artículo 41.1 que, “*los fabricantes, importadores y suministradores de maquinaria, equipos, productos y útiles de trabajo, están obligados a asegurar que éstos no constituyan una fuente de peligro para el trabajador*”. Asimismo, se obliga al empresario a utilizar los equipos de trabajo conforme a los fines y de forma recomendada por el fabricante (Artículo 41 LPRL).

Del mismo modo, se considerará fabricante a aquellas personas que modifiquen sustancialmente los productos ya comercializados, debiendo igualmente asumir las obligaciones correspondientes. Se considerarán modificaciones sustanciales aquellas modificaciones que cumplan con los tres criterios que a continuación se mencionan:

- 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.

A pesar de que la consideración de modificación sustancial no es del todo clara para todos los casos, se tiene como orientación todos aquellos cambios que no hayan sido previstos por el fabricante. Siendo esto así, en casos en los que, por ejemplo, el empresario se limite a actualizar el software conforme a las indicaciones previstas, no estaríamos ante un supuesto de modificación sustancial<sup>78</sup>.

Como ya hemos mencionado entre las obligaciones de los sistemas IA de alto riesgo, deben ser vigilados de manera efectiva por personas físicas, con el objetivo de prevenir o reducir al mínimo los riesgos para la seguridad y la salud, entre otros. Esta vigilancia debe cubrir los supuestos en los que el sistema IA se esté utilizando tanto conforme a su uso previsto, como al razonablemente previsible (Artículo 14.1 Reglamento IA). En este sentido, la obligación empresarial vuelve a ser la misma marcada por la LPRL, ya que, atendiendo al artículo 15.4 de esta ley, las medidas preventivas deben prever tanto las distracciones como las imprudencias no temerarias (o profesionales), que pudiera cometer el trabajador. Siendo esto así, las personas designadas

---

<sup>78</sup> RODRIGUEZ SANZ DE GALDEANO, Beatriz (2023). Op Cit. Pág. 68

para cumplir con esta función tendrán un nivel de alfabetización suficiente en materia de IA y dispondrán de los recursos necesarios para garantizar la supervisión eficaz del sistema.

Por otro lado, los implementadores de cualquier sistema IA destinado a interactuar con personas físicas, deben informar de manera clara, inteligible y oportuna a dichas personas físicas expuestas a un sistema de IA, de que esta interactuando con dicho sistema (excepto en las situaciones que resulte evidente). Del mismo modo, aquellos que utilicen reconocimiento de emociones o categorización biométrica, requerirán del consentimiento antes del tratamiento de datos personales<sup>79</sup>. Esto mismo venía ya establecido en el artículo 15.1 RGPD, donde se establece que los interesados tendrán derecho a obtener del responsable del tratamiento confirmación de si están tratando o no datos personales, así como concretamente en el apartado h, en el que se vuelve a hacer referencia a las decisiones automatizadas del artículo 22 RGPD. En último lugar, el empresario tendrá la obligación de incluir todas las medidas anteriormente mencionadas dentro de la Planificación de la Actividad Preventiva.

## **V. POSIBLES IMPACTOS NEGATIVOS DEL USO DE SISTEMAS DE IA EN EL TRABAJO**

Como ya hemos visto, el uso de sistemas de IA en las empresas puede ayudar a mejorar la eficacia de gestión del personal, asignación de tareas o incluso liberar a las personas trabajadoras de tareas penosas. A pesar de ello, la implementación de IA, así como la automatización de procesos, conllevarán otro tipo de consecuencias tanto en la forma de entender las relaciones laborales, como en las personas trabajadoras. Centrándonos en esta última, diversos estudios han demostrado que la automatización y la inteligencia artificial pueden reducir accidentes laborales, pero también pueden implicar un impacto negativo en la salud física y mental<sup>80</sup>.

En este sentido, es especialmente relevante el impacto atribuido a los factores psicosociales vinculados con la industria 4.0 sobre la salud mental del personal, constituyendo actualmente uno de los principales retos en el campo de la prevención de

---

<sup>79</sup> Artículo 52 Reglamento Inteligencia Artificial

<sup>80</sup> FERREIRA GRANADOS, Jackeline. "El impacto de la inteligencia artificial en los trabajadores despedidos por automatización de servicios" en *Revista CES Derecho*, 14(3), 62-81, 2023

riesgos laborales<sup>81</sup>. Se ha demostrado que el estrés, la discriminación, el aumento de la precariedad, los trastornos musculoesqueléticos y las posibilidades de intensificación de trabajo y pérdida de empleo asociados al uso de Inteligencia Artificial en el trabajo provocan riesgos psicosociales<sup>82</sup>.

Por otro lado, la pérdida de control y autonomía del trabajo son riesgos comúnmente reportados como consecuencia del uso de sistemas AIWM, ya que, en algunos casos, estos sistemas pueden llegar a asumir el control del trabajo. Asimismo, la mayoría de los sistemas algorítmicos y los basados en IA dictan como realizar el trabajo o las tareas, lo que puede resultar en una pérdida del control de su trabajo.

Por otro lado, ya hemos visto que son varios los sistemas diseñados para recopilación de datos, sean o no de carácter personal, de las personas trabajadoras. Siendo esto así, en algunos casos esta recopilación de datos se puede asumir como una invasión de la vida privada, sobre todo cuando se relaciona con una vigilancia abusiva. Esta sensación de invasión de la intimidad puede llegar a provocar estrés, ansiedad, presión de desempeño, entre otras. En relación con esta última idea, se dice que los sistemas IA generan presión de desempeño, por ejemplo, aumentando la velocidad o evaluando el ritmo de trabajo. Siendo esto así, la sensación de estar realizando el trabajo bajo supervisión<sup>83</sup>.

Por otro lado, economistas de la universidad de Oxford indican que el cambio tecnológico podría llegar a tener impacto sobre 702 ocupaciones. En Estados Unidos el 47% del empleo total tendrá modificaciones, en Reino Unido 15 millones de puestos de trabajo serán afectados y en estadísticas del Instituto Global McKinsey, 375 millones de personas trabajadoras tendrán que cambiar hacia nuevas ocupaciones<sup>84</sup>.

Asimismo, la eliminación de la mano de obra humana, se eliminarían también obligaciones empresariales asociadas a ella, como pueden ser el pago de la seguridad social, el cumplimiento de la jornada de trabajo, salarios, vacaciones, indemnizaciones, etc. Siendo esto así, los casos de implementación de IA que impliquen automatización de

---

<sup>81</sup> Parlamento Europeo (2022) "Resolución del Parlamento Europeo, de 5 de julio de 2022, sobre la salud mental en el mundo laboral digital [2021/2098(INI)]" Disponible en: [https://www.europarl.europa.eu/doceo/document/TA-9-2022-0279\\_ES.html](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0279_ES.html)

<sup>82</sup> MOORE, Phoebe. "The threat of physical and psychosocial violence and harassment in digitalized work". *International Labour Organization*, 2018. [http://oit.org/wcmsp5/groups/public/---ed\\_dialogue/---actrav/documents/publication/wcms\\_617062.pdf](http://oit.org/wcmsp5/groups/public/---ed_dialogue/---actrav/documents/publication/wcms_617062.pdf)

<sup>83</sup> MEGINO FERNÁNDEZ, Diego (2023). Op. Cit. Pag. 20

<sup>84</sup> BENEDIKT FREY, Karl y OSBORNE, Michael. "The future of employment: how susceptible are Jobs to computerisation?" Universidad de Oxford, 2013.

procesos y, en consecuencia, eliminación de la mano de obra, podrían llegar a generar una inestabilidad económica del sistema<sup>85</sup>.

Por todo ello, aunque existen beneficios claros, es necesario considerar cuidadosamente los efectos globales de la robótica y buscar soluciones que minimicen los impactos negativos en los trabajadores y la sociedad en general<sup>86</sup>.

## VI. CONCLUSIONES

Es innegable que la Inteligencia Artificial cada día tiene más presencia en nuestra sociedad, por lo que es inevitable que este aumento de presencia también se vea reflejado en el mundo de la empresa. Este nuevo cambio, al que actualmente nos referimos como “cuarta revolución industrial”, ha llegado para quedarse, por lo que al igual que pasó en las revoluciones anteriores, supondrá la integración y adaptación a una nueva realidad.

Aunque a nivel tecnológico y de desarrollo las posibilidades de la Inteligencia Artificial son infinitas, a nivel jurídico es imprescindible establecer unos límites que ayuden a que la evolución tecnológica no ponga en compromiso los derechos fundamentales de las personas. Es por ello que, con el fin de aprovechar los beneficios de la IA, sin olvidar los problemas y desafíos que implica, resulta necesaria una regulación, a menos a nivel europeo, como la que se propone en el Reglamento IA. Es importante tener como referencia que este Reglamento se desarrolla con el fin de que los sistemas IA en el mercado de la UE sean seguros, fiables y respeten la legislación vigente y los valores de la Unión, pero sin querer limitar ni obstaculizar el desarrollo tecnológico.

pesar de que la Inteligencia Artificial no es algo reciente, no es hasta 2018 cuando a nivel europeo se plantea la necesidad de regularla. Esto no ha sido, ni es, un proceso fácil, ya que se trata de un ámbito que evoluciona a un ritmo mucho más rápido del que la legislación puede hacerlo, por lo que, al igual que ya ha sucedido, será necesario seguir realizando cambios que permitan reflejar y cubrir mejor esta realidad.

Teniendo como referencia que uno de los objetivos principales del Reglamento es el de proteger los derechos fundamentales de los y las ciudadanas de la Unión, se propone

---

<sup>85</sup> FERREIRA GRANADOS, Jackeline (2023). Op. Cit. Pag. 71

<sup>86</sup>GOÑI SEIN, José Luis. “Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo”. *Documentación Laboral*, 2 (117), 57-72, 2019

para su regulación un análisis basado en los riesgos para estos derechos. Siendo esto así, se proponen cuatro categorías: prácticas inadmisibles, de alto riesgo, riesgo limitado y riesgo mínimo.

Como vemos, a día de hoy, en la Unión Europea se considera necesario catalogar determinadas prácticas como prohibidas. Este tipo de prácticas suponen una amenaza real para la seguridad, la vida y los derechos de las personas, por lo que, frente al desarrollo tecnológico, se persigue priorizar la protección de las personas.

A diferencia de estos, en la siguiente categoría se clasifican los sistemas, a pesar de suponer un alto riesgo para la seguridad, salud o derechos fundamentales, sí están permitidos. De nuevo, dada la capacidad de generar daño que estos sistemas pueden llegar a tener, es imprescindible que cumplan con una serie de requisitos y obligaciones que aseguren su seguridad. Asimismo, hay determinados ámbitos en los que, además de ser muy probable la materialización del daño, en caso de que este ocurriera, los derechos fundamentales se podrían ver gravemente afectados. En este sentido, nos afecta concretamente el empleo.

En último lugar, las prácticas de riesgo limitado y riesgo mínimo, como su propio nombre indica, serán las menos invasivas y perjudiciales para los derechos de las personas. Siendo esto así, el Reglamento reserva para ellas una mayor flexibilidad y menor exigencia a la hora de cumplir con obligaciones. A pesar de ello, destaca especialmente la necesidad de transparencia, para que el usuario sea consciente de la interacción con este tipo de sistemas.

Se debe tener presente que el Reglamento ha sido desarrollado con el objetivo de poder ser aplicado en múltiples ámbitos, entre los que también se recoge la empresa y, consecuentemente, la seguridad y salud en el trabajo. A pesar de ello, resulta complejo englobar y desarrollar circunstancias que puedan ser de aplicabilidad en cada contexto en el que se pueda utilizar IA, por lo que, a la hora de clasificar un sistema, es necesario entender todas las implicaciones que este pudiera llegar a tener. Siendo esto así, nos encontramos ante la posibilidad de que, un mismo sistema IA pueda ser categorizado en un nivel de riesgo u otro, atendiendo a las características con las que este trabaje.

Como ya hemos mencionado, la IA tiene infinidad de aplicaciones desde el punto de vista técnico y, en algunos casos, la realidad puede llegar incluso a superar a la ficción. Siendo esto así, aunque la ficción nos permita plantear sistemas como el mencionado por

Veale y Zuiderveen Borgesius para aumentar el rendimiento de las personas, hay prácticas que de cualquier forma, probablemente siempre generarían más perjuicio que beneficio en la persona.

En relación a la generación de perjuicio, es precisamente una de las cosas que el Reglamento pretender evitar, a pesar de que en algunos casos, resulte inevitable. En este sentido, volvemos de nuevo a la idea de que el Reglamento ha sido planteado para poder ser utilizado, de forma indistinta en todos los ámbitos. Concretamente, centrándonos en la necesidad de “provocar un daño significativo”, además de ser intencionado, que se establece para los sistemas prohibidos. Resulta contradictorio pensar que, en un ámbito en el que precisamente el objetivo es el de evitar un daño para la seguridad y salud de la persona trabajadora, se aplique una herramienta destinada a provocar un daño intencionadamente.

Del mismo modo, aunque algunos sistemas IA sean muy útiles para optimizar procesos, desde el punto de vista tanto de los Recursos Humanos como de la Prevención de Riesgos Laborales, no se puede olvidar que el elemento central es la persona trabajadora, la cual tiene, ante cualquier situación y contexto, unos derechos. De esta manera, aunque la decisión de establecer determinados filtros sea a través de una persona humana, es necesario también que las decisiones, a posteriori, sean igualmente supervisadas.

Asimismo, además de tener presente todo lo que el Reglamento IA establece sobre, concretamente, los sesgos, decisiones con un trasfondo discriminatorio o la protección de datos, se debe tener también siempre presente el marco legal que exista en cada país en relación a estos aspectos, En este sentido, es imprescindible completar lo establecido en el Reglamento con la Ley 15/2022 para la igualdad y no discriminación y el Reglamento General de Protección de datos.

Las obligaciones establecidas por el Reglamento van especialmente dirigidas a los proveedores y a implementadores o usuarios, reflejado en la figura del empresario en nuestro caso. Siendo esto así, además de ser necesario cumplir con todos los requisitos y obligaciones para asegurar que los sistemas IA introducidos en el mercado sean seguros, hay que sumarle también la obligación, que ya venía existiendo, de que el empresario ponga a disposición de las personas trabajadoras elementos de trabajo seguros.

Por último, y volviendo a la base del Reglamento, desde el punto de vista de la PRL, a la hora de integrar en la empresa cualquiera de estos sistemas, se debe tener en cuenta, además del cumplimiento del Reglamento, todos los perjuicios y beneficios que este tipo de herramientas provocarían en las personas. Por ello, los sistemas de inteligencia artificial que vayan a ser utilizados en la empresa, deberán también estar incluidos dentro de la Planificación de la Actividad Preventiva, además de identificar en la Evaluación de Riesgos aquellos riesgos, especialmente a nivel psicosocial, que pudieran generarse.

## VII. BIBLIOGRAFÍA

- ALLEJO NOGUERA, Franco Fernando, RUBIO ENDARA, Omar Washington y TELLO MOREIRA, José Antonio. “Implementar el Uso de la Inteligencia Artificial para Detectar el Comportamiento del Trabajador en la Prevención de Accidentes Laborales en la Empresa”. *Dominio de las Ciencias*, 8(1), 21.
- BENEDIKT FREY, Karl y OSBORNE, Michael. “The future of employment: how susceptible are Jobs to computerisation?” Universidad de Oxford, 2013.
- Comisión Europea (2022) “Propuesta de marco normativo sobre inteligencia artificial” <https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai>
- COTINO HUESO, Lorenzo “Sistemas de inteligencia artificial con reconocimiento fácil y datos biométricos. Mejor regular bien que prohibir mal” en *El Cronista del Estado y Democrático de Derecho*, núm. 100, 2022
- DAMASIO, Antonio (2006) “El error de Descarte. La emoción, la razón y el cerebro humano”. Barcelona
- EU-OSHA, “Artificial intelligence for worker management: implications for occupational safety and health – Executive Summary” Disponible en <https://osha.europa.eu/es/publications/summary-artificial-intelligence-worker-management-implications-occupational-safety-and-health>
- EU-OSHA, “Equipos de protección individual inteligentes: protección inteligente de cara al futuro” Disponible en: <https://osha.europa.eu/es/publications/smart-personal-protective-equipment-intelligent-protection-future>
- EU-OSHA, “Trabajo en plataformas digitales: consecuencias para la salud y seguridad en el trabajo” Disponible en: <https://osha.europa.eu/es/publications/digital-platform-work-implications-occupational-safety-and-health>
- FEMEVAL, Guía de Realidad Virtual y Realidad Aumentada, disponible en [https://www.femeval.es/dam/jcr:57a1b2aa-982b-40bd-b0f0-3b3d45bc162b/GUIA\\_RV\\_RA\\_link.pdf](https://www.femeval.es/dam/jcr:57a1b2aa-982b-40bd-b0f0-3b3d45bc162b/GUIA_RV_RA_link.pdf)
- FERREIRA GRANADOS, Jackeline. “El impacto de la inteligencia artificial en los trabajadores despedidos por automatización de servicios” en *Revista CES Derecho*, 14(3):62-81, 2023.
- GALINDO GARCÍA, Javier. ¿Sirve la realidad virtual para prevenir riesgos laborales? Disponible en <https://www.asepeyo.es/blog/seguridad-laboral/realidad-virtual-para-prevenir-riesgos-laborales/>
- GAMERO CASADO, Eduardo. “El enfoque europeo de Inteligencia Artificial” en *Revista de Derecho Administrativo*, núm. 20, 2021, págs. 268-289
- GOÑI SEIN, José Luis. “Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo”. *Documentación Laboral*, 2 (117), 57-72, 2019
- IBM, Cómo las tecnologías de la Industria 4.0 están cambiando la fabricación. <https://www.ibm.com/es-es/topics/industry-4-0>
- KELLY-LYTH, Aislinn. “The AI Act and algorithmic management”, Universidad de Harvard disponible en <https://cllpj.law.illinois.edu/content/dispatches/2021/Dispatch-No.-39.pdf>

- LLORENS ESPADA, Julen. Límites al uso de la Inteligencia Artificial en el ámbito de la Salud Laboral, LA LEY Soluciones Legales, Madrid, 2023.
- MACÍAS GARCÍA, María del Carmen. (2022) “La inteligencia artificial para el entorno laboral. Un enfoque en la predicción de accidentes”. *e-Revista Internacional de la Protección Social*, 7 (1), 84-101.
- MARTÍNEZ, Fredy, HERNÁNDEZ, César y GIRAL, Diego “Sistema integrado de reconocimiento de emociones para interacción hombre-máquina”. *Información tecnológica*, 34(1), 117-128.
- MEGINO FERNÁNDEZ , Diego. “La formación como principio y fin de la acción preventiva frente a los riesgos psicosociales derivados de la digitalización y la automatización” en *Lan Harremanak-Revista de Relaciones Laborales*, núm. 49, 2023.
- MIRA PÉREZ, Paula. “Prevención de Riesgos Laborales en la Industria 4.0” Universidad de Valladolid (2020)
- MOORE, Phoebe. “The threat of physical and psychosocial violence and harassment in digitalized work”. *International Labour Organization*, 2018. [http://oit.org/wcmsp5/groups/public/---ed\\_dialogue/---actrav/documents/publication/wcms\\_617062.pdf](http://oit.org/wcmsp5/groups/public/---ed_dialogue/---actrav/documents/publication/wcms_617062.pdf)
- MOORE, Phoebe. “Inteligencia artificial en el entorno laboral. Desafíos para los trabajadores”. *Universidad de Leicester*, 2020. <https://www.bbvaopenmind.com/articulos/inteligencia-artificial-en-entorno-laboral-desafios-para-trabajadores/>
- RODRÍGUEZ SANZ DE GALDEANO, B. y EGÚSQUIZA BALMASEDA, M. A. (dir.): *Obligaciones y responsabilidades*. Tirant lo Blanch, Valencia, 2023
- Observatorio Nacional de Tecnología y Sociedad (2023) “Uso de inteligencia artificial y big data en las empresas españolas”, 2023.
- OIT, “Perspectivas Sociales y del Empleo en el Mundo. El papel de las plataformas digitales en la transformación del mundo del trabajo”. Disponible en: [https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms\\_771675.pdf](https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_771675.pdf)
- PONCE, Aida. “The AI Regulation: Entering an AI Regulatory Winter? Why An Ad Hoc Directive on Ai in Employment Is Required” European Trade Union Institute (ETUI) Research Paper. Disponible en: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3873786](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873786)
- Portal Administración Electrónica (2023) “Ley de Inteligencia Artificial: el Consejo y el Parlamento Europeo llegan a un acuerdo sobre las primeras normas para regular la IA en el mundo” [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Actualidad/pae\\_Noticias/Anio2023/Diciembre/Noticia-2023-12-11-Ley-de-inteligencia-artificial-el-Consejo-y-el-Parlamento-Europeo-llegan-a-un-acuerdo-sobre-las-primeras-normas-en-el-mundo-para-regular-la-Inteligencia-Artificial.html](https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2023/Diciembre/Noticia-2023-12-11-Ley-de-inteligencia-artificial-el-Consejo-y-el-Parlamento-Europeo-llegan-a-un-acuerdo-sobre-las-primeras-normas-en-el-mundo-para-regular-la-Inteligencia-Artificial.html)
- SALGUERO-CAPARRÓS, Francisco Miguel, “Seguridad laboral e industrial: nuevas tecnologías en la Industria 4.0”. Universidad de Málaga

- Sociedad Española de Salud y Seguridad en el Trabajo (2021) “El Uso de Sistemas de Inteligencia Artificial Para Reducir la Siniestralidad en el Trabajo”. Disponible en <https://www.sesst.org/e-prevenir-a-predecirel-uso-de-sistemas-de-inteligencia-artificial-para-reducir-lasiniestralidad-en-el-trabajo/>
- TAPIA CEDEÑO, STEFANÍA JOHANNA. “La inteligencia artificial como herramienta complementaria en la investigación y educación: responsabilidad ética y humana” en Revista Unidad Sanitaria XXI, 3(8).
- VEALE, Michael y ZUIDERVEEN BORGESIUS, Frederik. “Demystifying the Draft EU Artificial Intelligence Act”, en *Computer Law Review International*, núm 22 (4), 2021