Facultad de Ciencias Jurídicas - Unidad AA3 Jurídicas
Zientzia Juridikoen Fakultatea - LA3 Juridikoen Unitatea

upna
Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Edificio de Las Encinas / Arteak eraikina
Campus de Arrosadia / Arrosadiko Campusa
31006 - Pamplona-Iruñea
Tel. (+34) (+34) 948 16 6203
facultad.cienciasjuridicas@unavarra.es

TRABAJO FIN DE ESTUDIOS / IKASGAIEN AMAIERAKO LANA

MÁSTER UNIVERSITARIO EN PREVENCIÓN DE RIESGOS LABORALES

IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN MATERIA DE PREVENCIÓN DE RIESGOS LABORALES Y PROPUESTAS NORMATIVAS DE ACTUACIÓN

Joao Paulo Araujo Monteiro

DIRECTOR / ZUZENDARIA

Beatriz Rodríguez Sanz de Galdeano

Pamplona / Iruñea

09 de septiembre de 2022

Resumen

El progreso tecnológico de los sistemas de Inteligencia Artificial (IA), ha llevado a la Unión Europea (UE) a elaborar una propuesta de regulación de la IA que pretender establecer un Nuevo Marco Normativo en coherencia con el acervo social europeo. Esta propuesta centrada en el ser humano pretende impulsar el desarrollo de la tecnología sin dejar atrás la seguridad y salud, y los derechos de trabajadores y usuarios.

En este trabajo se presentarán las tecnologías más disruptivas en materia de IA, realizando un razonamiento sobre los retos que estos sistemas proponen en el ámbito de prevención de riesgos laborales, de cara a su desarrollo y utilización. A partir de este estudio se tratará de analizar como la UE propone, a través de la Ley de IA, resolver estas cuestiones, cómo esta nueva normativa conecta con la propuesta de actualización de la nueva Directiva de Máquina y con la propuesta de Responsabilidad Civil en materia de inteligencia artificial.

Palabras clave: *Inteligencia Artificial, Robot, Internet de las cosas, Seguridad del producto, Responsabilidad Civil IA.*

Abstract

In view of the technological progress of Artificial Intelligence (AI) systems, the European Union (EU) has drafted a proposal for the regulation of AI that aims to establish a New Regulatory Framework in coherence with the European social acquis. This human-centered proposal aims to boost the development of technology without leaving behind health and safety, and the rights of workers and users.

This work will present the most disruptive technologies in the field of AI, making a reasoning on the challenges that these systems propose in the field of occupational risk prevention, facing its development and use. From this study we will try to analyze how the EU proposes, through the AI Law, to solve these issues, how this new regulation connects with the proposed update of the new Machine Directive and with the proposal of Civil Liability in artificial intelligence.

Key words: *Artificial Intelligence, Robot,* Internet of Things, Civil Liability, AIA.

Índice

I. INTRODUCCIÓN

La Revolución Industrial marcó un antes y un después en la historia de la humanidad. En especial porque impactó en toda la esfera social y significó la creación de innovaciones tecnológicas y científicas que supusieron una ruptura con las estructuras socioeconómicas existentes hasta el momento.

Se pueden distinguir cuatro etapas de la Revolución Industrial, son ellas:

1. Primera Revolución: fue un proceso de profundas transformaciones económicas, sociales, culturales y tecnológicas que se desarrolló entre 1760 y 1840, y tuvo su origen en Inglaterra. Estableció la mecanización del sistema de producción, con la incorporación de la máquina de vapor, el ferrocarril, energía hidráulica y mecanización.
2. Segunda Revolución: se inicia a mediados del siglo XIX, cuando los avances tecnológicos y científicos empiezan a tomar una forma más compleja. Con ello, se fue abriendo camino a distintos recursos naturales, indisponibles o poco útiles hasta ese momento que permitieron lograr un aumento de la energía disponible que, además, se diversificó, como la electricidad y su aplicación a la industria, al transporte y a la vida doméstica, o el petróleo. En consecuencia, se impulsó de manera importante el manejo del acero, que era una materia prima fundamental para la construcción y la fabricación de nuevas máquinas y herramientas, y permitió la producción en masa, creación de las cadenas de montaje etc.
3. Tercera Revolución: se sostiene sobre las nuevas tecnologías de la información y la comunicación ubicadas a mediados del siglo XX, que han posibilitado consumar un modelo de automatización de los procesos. Igualmente, la informática ha proporcionado el desenvolvimiento de energías renovables. Como resultado de las potencialidades de estos dos elementos actuando conjuntamente, se obtuvieron grandes cambios en diversas áreas. Nunca se había llegado a unas cotas tan altas de interactividad e intercomunicación, al tiempo que las innovaciones en materia energética podían significar un cambio tan sustancial como el que se prevé con el desarrollo y explotación de fuentes renovables de energía.

4. Cuarta Revolución: El último capítulo, hasta la fecha, de las revoluciones industriales que la humanidad ha presenciado. Algunos de los fundamentos sobre los que se levanta esta revolución son:

    - El internet de las cosas (IoT), definida como "es un sistema conformado por diversos dispositivos únicos e identificables, conectados a una red y que tienen la capacidad de enviar datos sin necesidad de intervención humana directa"[1].
    - Robótica y dispositivos conectados.
    - Los sistemas ciberfísicos, que combinan máquinas físicas y tangibles con procesos digitales.
    - La fábrica 4.0 (ciber fábrica o *smart-industries*) y fabricación aditiva, esta se define como el "proceso de unión de materiales para fabricar piezas u objetos a partir de datos de modelos 3D, generalmente capa a capa, en oposición a métodos de fabricación mediante eliminación de material y de conformado"[2].
    - En definitiva, los sistemas de Inteligencia Artificial (IA).

La estructura actual del entorno del trabajo y el mercado laboral serán algunas de las áreas donde el impacto será más importante. Los sistemas de IA basados en el aprendizaje automático[3] y otras técnicas están cada vez más presentes en nuestras vidas. Las empresas privadas utilizan los algoritmos de aprendizaje automático en casi todos los ámbitos, incluidos los servicios financieros, la fabricación, la agricultura, la ingeniería, el transporte, las telecomunicaciones, el comercio minorista, los viajes, la logística y la atención sanitaria.

---

[1] FEMEVAL, *Guía de Sistemas IoT en Prevención de Riesgos Laborales*, disponible en https://www.femeval.es/dam/jcr:be830229-384d-45fd-909e-4a60d2ef5b71/GUIA%20IOT.pdf

[2] FEMEVAL, *Guía de Fabricación Aditiva en Prevención de Riesgos Laborales*, disponible en https://www.femeval.es/dam/jcr:aa78cfcc-5068-4abd-8999-9c6c1d201e4d/GUIA-FABRICACION-ADITIVA.pdf

[3] BUCHANAN, B. AND MILLER, T., *Machine Learning for Policymakers*: *What It Is and Why It Matters,* Harvard Kennedy School, Belfer Center for Science and International Affairs, June 2017, disponible en https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf

Muchos de estos sistemas tienen el potencial de mejorar nuestras vidas, así como el bienestar económico y social general. Los sistemas impulsados por la IA pueden dar lugar a mejores servicios sanitarios, sistemas de transporte más seguros y limpios, mejores condiciones de trabajo, mayor productividad y nuevos productos, servicios y cadenas de suministro innovadores.

Sin embargo, como ocurre con toda tecnología disruptiva, los sistemas de IA no sólo conllevan beneficios, sino también riesgos sustanciales, lo que plantea una amplia variedad de retos éticos y legales. Los sistemas de IA tienen el potencial de dañar de forma impredecible la vida, la salud y la propiedad de las personas. También pueden afectar a los valores fundamentales en los que se basan las sociedades occidentales, dando lugar a violaciones de los derechos fundamentales de las personas, incluidos los derechos a la dignidad humana y a la autodeterminación, a la privacidad y a la protección de los datos personales, a la libertad de expresión y de reunión, a la no discriminación o al derecho a un recurso judicial efectivo y a un juicio justo, así como a la protección de los consumidores.

Incorporar la tecnología como herramienta cotidiana en el lugar de trabajo, el hogar o el transporte invita a la reflexión y presenta desafíos hasta ahora desconocidos e inexplorados. El gran reto para los próximos años será minimizar los impactos negativos de la Industria 4.0 y maximizar los positivos. Un aspecto fundamental que debe ser priorizado, es la capacidad de regular adecuadamente todo el proceso y su impacto.

El objetivo de este trabajo investigativo es analizar el régimen legal en materia de obligaciones y responsabilidades en marco europeo en el ámbito de seguridad del producto por la incorporación de la IA y los desafíos que se enfrenta la UE para establecer un nuevo marco normativo.

II. APROXIMACIÓN A LAS APORTACIONES DE LA INTELIGENCIA ARTIFICIAL EN MATERIA DE PRL

Desde siempre el mundo del trabajo se enfrenta a cambios constantes. Los desarrollos e innovaciones tecnológicas han sido y siguen siendo los principales impulsores de los cambios en los puestos de trabajo y las tareas laborales. Los sistemas basados en la IA no son del todo nuevos; sin embargo, el desarrollo de las Tecnologías de la Información y la Comunicación (TICs) y de los algoritmos adaptativos, facilitado por el extraordinario aumento de la potencia de cálculo en los últimos años, ha propiciado

un enorme aumento de la disponibilidad y el rendimiento de las aplicaciones basadas en la IA. Además, la aparición y el rápido desarrollo de nuevas tecnologías, como los sistemas robóticos que pueden interactuar estrechamente con los seres humanos, han hecho resurgir el debate sobre el potencial de automatización de los puestos de trabajo y las tareas, así como sus consecuencias para la seguridad y la salud en el trabajo.

Para comprender este proceso de transformación, que esta englobado en lo que es conocido como la cuarta revolución industrial, se debe empezar por tener claro en qué consiste la Industria 4.0. La respuesta consiste en la digitalización y en las llamadas tecnologías habilitadoras, que sustentan esta transformación. Esta industria es aquella con el enfoque que busca interconectar todas las unidades de producción de una empresa. Esto se refleja en el hecho de que la base de esta industria son los datos, que son el mecanismo para hacer funcionar gran parte de las tecnologías habilitadoras y así alcanzar una industria inteligente.

Para ello, se pueden distinguir dos partes que se complementan dentro de los habilitadores digitales. Por un lado, tecnologías que permiten recopilar información, procesarla realizando análisis y aprender de los datos, por ejemplo, podemos mencionar *Big Data,* que se trata de una "cantidad muy grande de datos, mucho mayor de lo que puede analizarse hoy en día en un solo ordenador, procedentes de diferentes fuentes y en diferentes formatos, a menudo no estructurados"[4] o *Cloud Computing,* en español la nube, que es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software etc.

Por el otro, las herramientas físicas que permiten la realización de acciones basadas en el aprendizaje a partir de datos capturados por los sensores y procesados por la tecnología como la IA o mediante la simulación de entornos virtuales, como la realidad virtual o aumentada, etc.

La tendencia que trae la industrial 4.0 es hacia la automatización total de la fabricación. La automatización se basa en los sistemas ciberfísicos capaces de tomar decisiones descentralizadas y cooperar entre sí y con otros a través del Internet de las

[4] EUROPEAN COMMISSION (December 2016), *Study on Big Data in Public Health*, Telemedicine and Healthcare, disponible en https://wayback.archive-it.org/12090/20170117023306/https://ec.europa.eu/health/sites/health/files/ehealth/docs/bigdata_report_en.pdf.

Cosas, impulsado por la nube, la fabricación aditiva a través de impresoras 3D, y el apoyo indispensable de la IA y el *Big Data*, como tecnologías clave para convertir la ingente cantidad de datos, que se está comenzando a generarse, en conocimiento y utilizarse de manera efectiva en la toma de decisiones. Armados con estas tecnologías, se avanza hacia fábricas inteligentes, donde las empresas podrán crear redes inteligentes que se controlen a sí mismas a lo largo de la cadena de valor.

Todo esto tendrá un gran impacto en la seguridad y salud en el trabajo, dados los cambios en la forma en que se está realizando el trabajo en la actualidad. Se trabaja conectado desde cualquier sitio, con herramientas digitales, en la nube, compartiendo tareas sea con compañeros de trabajo o con robots, además la automatización y digitalización de procesos también modifica el modelo de producción, quitando a personas de tareas de poco valor añadido o con alta carga de riesgos laborales, por robots, permitiendo la creación de puestos de control de estos equipos, más cualificados y con menos riesgos para la seguridad y salud.

Se detallará algunas de estas nuevas tecnologías disruptivas y se observará las ventajas de su implantación y las posibles consecuencias a nivel de prevención de riesgos laborales (PRL).

1. Robots Avanzados

La definición de la Real Academia Española (RAE) del término robot, aclara que es una "Máquina o ingenio electrónico programable que es capaz de manipular objetos y realizar diversas operaciones". Por otro lado, existen otras definiciones bastante extendidas sobre lo que es un robot, entre las cuales se puede destacar la que engloba por completo sus características, especificando que "se trata de un sistema que es capaz de percibir el entorno o contexto en el que se encuentra, que puede procesarla información para planificar una determinada actuación y ejecutarla"[5]. En este último concepto se comprenden tanto robots-maquinas como entidades de IA.

Los robots-máquinas puede ser lo que se conoce como los brazos mecánicos, que ensamblan piezas en una línea de montaje, máquinas que actúan de forma autónoma a partir de programas de ordenador. En el caso de las entidades de IA, se tratan de

[5] CALO, R. "Robotics and the Lessons of the Cyberlaw", 103, Cal. L. Rev. 2015, p.513 y ss, *UW Law Digital Commons*, disponible en https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1022&context=faculty-articles

algoritmos, que responden a una finalizada prediseñada o que pueden ser capaces de tomar decisiones autónomas a partir de la información, que van en cada momento, procesando y que les suministra permanentemente al estar conectados a otras máquinas o base de datos por medio de la tecnología empleada en el "Internet de las cosas". Es el caso de los drones o vehículos autónomos.

Los robots avanzados, o lo que para este estudio es lo mismo, los "robots inteligentes", teniendo en cuenta la Resolución del Parlamento Europeo, se caracterizan por reunir los siguientes requisitos:

- Capacidad de adquirir autonomía mediante sensores y/o intercambio de datos con su entorno y el intercambio y análisis de dichos datos.
- Un soporte físico mínimo.
- Capacidad de adaptar su comportamiento y acciones al entorno.
- Inexistencia de vida en sentido biológico.
- Capacidad de autoaprendizaje a partir de la experiencia y la interacción.

Para que un sistema tenga la consideración de robot es necesario que realice tres actividades básicas; En primer lugar, "percibir", es decir ser un generador de información de su entorno para lo cual dispone de los sensores. En segundo lugar, ser capaz de "planificar", es decir seleccionar acciones o determinar situaciones o comportamientos que pueden ocurrir, en base a la información percibida, esta sería la parte de los programas que gestionan los datos y permiten la toma de decisión. Y por último "actuar", esto es, ejecutar el plan trazado, normalmente utiliza la parte física de la maquinaria para realizar las acciones.

En estas acepciones aparentemente sencillas se ocultan rasgos que pueden inquietar y limitar su generalización en el entorno de trabajo, entre los cuales está la complejidad que habitualmente se vincula a la impredictibilidad, esto es, la dificultad para predecir comportamientos futuros y la posibilidad de asumir tareas humanas.

En este último aspecto se encuentra básicamente el elemento diferenciador en comparación con las revoluciones anteriores, que mientras las máquinas antiguas reemplazaban fundamentalmente la fuerza muscular, las nuevas pueden sustituir a la capacidad intelectual y las habilidades cognitivas. En consecuencia, sus repercusiones se dejarán sentir no sólo entre los trabajadores poco cualificados sino también entre aquellos

con mayor grado de cualificación y especialización, incidiendo en un gran número de sectores al mismo tiempo. En esta tesitura, resulta patente que también tendrá importantes repercusiones en el terreno de la seguridad y salud de los trabajadores.

En este sentido los robots inteligentes, tanto los robots aislados como los colaborativos con los humanos, estos conocidos como Cobots, tienen una gran capacidad de librar a los trabajadores de las actividades más gravosas, peligrosas o tóxicas y su enorme potencial para mejorar la seguridad en el entorno laboral. Se suele poner como ejemplo la utilización de exoesqueletos, que permiten desarrollar trabajos con menos esfuerzo físico, con beneficios contrastados frente a los riesgos de trastornos musculo esqueléticos, además permite la mayor integración de personas con cierta discapacidad, o simplemente robots que liberan a los trabajadores de tareas monótonas o repetitivas suprimiendo el riesgo de imprudencia profesional.

Asimismo, los robots también tienen la función de sustituir a los trabajadores en tareas que exijan acceder a zonas peligrosas o con alto riesgo de exposición a sustancias contaminantes, como pueden ser los agentes químicos o biológicos, con atmosferas explosivas, en instalaciones nucleares y similares. En contrapartida, también preocupa los riesgos que se pueden derivar de la propia expansión de la robótica, en especial en combinación con la IA, el riesgo de alienación y deshumanización de las tareas que se queden reducida a la supervisión al robot o al proceso productivo y los accidentes o incidentes provocados por los robots, además del sometimiento de las personas a las decisiones del robot, a sus ritmos de trabajo.

La flexibilidad de la fabricación en la Industria 4.0 necesitará robots capaces de interactuar con el entorno, con los productos fabricados y con las personas. Para lograr este objetivo será necesario que se superen algunos desafíos en vista a la introducción de los robots inteligentes en las empresas, como pueden ser:

- Integración progresiva de las nuevas tecnologías robóticas en los marcos legislativos.
- Un aspecto crucial para garantizar el éxito de una colaboración persona-robot, es la predictibilidad o facilidad para predecir cada uno de los siguientes pasos, lo que va asociado a una mayor y mejor señalización por el robot de sus intenciones hacia los humanos con los que interactúa.

2. Drones

La palabra "*drone*" viene del inglés que significa "zángano" o "abeja macho". Aunque su uso inicial fue básicamente direccionado al ámbito militar, en la actualidad los drones tienen inúmeras utilidades, desde tareas de inspecciones, como de control, sea en sectores como la agricultura como en la seguridad pública o privada.

Se definen los drones como un sistema aéreo no tripulado y aeronave controlada de forma remota. En España el marco normativo para esta tecnología aparece en el año 2017 con el Real Decreto (RD) 1036/2017, de 15 de diciembre, de aeronaves pilotadas por control remoto (RPAs), teniendo conexión con la normativa de PRL. Dicho RD estuvo vigente hasta el 1 de enero de 2022, a partir de esta fecha la normativa de drones que se aplica en España son los Reglamentos Europeos RE 2019/947 y RD 2019/945

A partir de la aplicación del Reglamento Delegado 2019/945, se estandarizan los requisitos y especificaciones técnicas que deben incorporar, de manera obligatoria, los drones destinados a las operaciones bajo categoría abierta, específica o certificada. El Reglamento de Ejecución 2019/947 establece tres categorías operacionales diferentes, atendiendo al nivel de riesgo de la operación en sí misma, que son:

- Categoría Abierta: se engloban los vuelos de **bajo riesgo**, para los que no se requerirá autorización previa ni tampoco declaración por parte del operador. Se regulan prohibiciones como, prohibición de sobrevuelo de grupos de personas, no se autoriza el transporte y/o arrojo de materiales o mercancías peligros, ni operaciones autónomas. También existen algunos requisitos que se deben cumplir en esta categoría como la edad mínima del piloto, que es de 16 años, el registro del operador, aprobar una formación teórica online y examen, la altura máxima de operación será de 120 metros, siempre mantener las aeronaves no tripuladas o UAS del inglés "*Unmanned Aerial Systems"* en la línea de visión etc.
- Categoría Específica: se aplica a las operaciones que no encajan dentro de la categoría abierta, por razones de riesgo:
    - Los vuelos son más allá de la línea de visión (vuelos BVLOS).
    - Operaciones de más de 120 metros de altura.
    - Drones de más de 25 Kg.
    - Vuelos urbanos con drones de más de 4 kg o sin marcado CE.

- Arrojo de materiales.
- Vuelo sobre aglomeraciones de personas, etc.

Se mantiene el requisito de la edad mínima y del registro del operador, además es necesario un estudio SORA, que se trata de una evaluación de riesgos de la operación[6]. Asimismo, si el vuelo ocurre fuera de los escenarios estándar (STS), el operador del dron deberá estar en posesión de una autorización operacional.

- Categoría Certificada: "Para una operación estar considerada dentro de esta categoría se debe cumplir con los siguientes requisitos generales:
  - Drones certificados bajo el Reglamento Delegado UE 2019/945.
  - Sobrevolar reuniones de personas con un UAS de más de 3 metros de envergadura.
  - Al sobrevolar aglomeraciones de personas transporten mercancías peligrosas con alto riesgo en caso de accidente; o cuando implique el transporte de personas.
  - Si el Estudio de Seguridad (SORA) indica necesidad de certificación del UAS, del operador y la obtención de la pertinente licencia de piloto.

  Las normas detalladas relativas a la categoría certificada aún están en desarrollo a nivel de la UE"[7].

Como en cualquier actividad, puesto de trabajo o profesión, los pilotos, observadores, reparadores y mantenedores de drones están sometidos a determinados riesgos que deben evaluarse y controlarse, teniendo en cuenta la legislación de PRL.

El autor Juan Carlos Bajo[8] realiza un análisis desde el punto de vista de la PRL, sobre aspectos que se deben tener en consideración que determinan las diferentes normativas aplicables:

---

[6] De conformidad con el Art. 11 del Reglamento de ejecución 947/2019.

[7] ON AIR, "Nuevo reglamento europeo de drones 2021" disponible en https://www.oneair.es/nuevo-reglamento-europeo-drones/#947 consultado en septiembre 2022.

[8] BAJO, J.C. "El uso profesional de los drones y la prevención de riesgos laborales" en Revista web MC Salud Laboral, abril 2021, págs. 18 a 23, disponible en https://prevencion.mc-mutual.com/articulos/-/asset_publisher/gPV7bp1C7xJS/content/el-uso-profesional-de-los-drones-y-la-prevencion-de-riesgos-laborales.

a) La empresa operadora como empresario: A los efectos de la legislación preventiva, la empresa operadora tendrá la consideración de empresario y por tanto deberá cumplir con todas sus obligaciones al respecto.

b) El piloto y observadores como trabajadores: Los pilotos y observadores del vuelo son trabajadores con todos los derechos y deberes que le corresponden.

c) Evaluación de riesgos: Como cualquier actividad profesional, ésta deberá ser evaluada de acuerdo con la Sección 1.ª (Evaluación de los riesgos) del Reglamento de los Servicios de Prevención. Es importante tener en cuenta que el entorno es diferente en cada uno de los escenarios de vuelo, por lo que, además de la evaluación general, se deberá realizar una evaluación específica para cada escenario de vuelo en función del entorno, independientemente de la evaluación de cada escenario de acuerdo con la normativa aérea.

d) Formación: Los pilotos y observadores, además de la formación obligatoria establecida en la legislación aérea, en particular en los Reglamentos Europeos, RE 2019/947 y RD 2019/945, deben tener formación desde un punto de vista preventivo de conformidad con el art. 19 de la Ley de Prevención de Riesgos Laborales (LPRL) en relación con los riesgos específicos del puesto.

e) El dron como equipo de trabajo: Los drones, a efectos del RD 1215/97, son equipos de trabajo puestos a disposición del trabajador, por lo que se deben cumplir todos los requisitos establecidos en el dicho RD. Por otra parte, el Reglamento Delegado de la Comisión (2019/945) indica que el drone debe cumplir con la Directiva 2006/42/CE (RD 1644/2008) en aquellos aspectos no relacionados con la seguridad aérea, debiendo el drone disponer de marcado CE con las características definidas en el reglamento delegado.

f) Equipos de protección individual: El piloto deberá contar con los equipos de protección individual acordes con las actividades que va a realizar de forma general, así como aquellos necesarios en función de cada uno de los escenarios de vuelo (ruido, caídas de objetos, calzado, etc.)

g) Vigilancia de la salud: El piloto, en virtud del Reglamento (CE) n.º 216/2008 del Parlamento Europeo y del Consejo, y en relación con los certificados médicos para la licencia de piloto de aeronave ligera, deberá disponer de un certificado de aptitud médica

aérea independientemente del reconocimiento médico que, como trabajador, deba realizarse de conformidad con el art. 22 de la LPRL.

h) Coordinación de actividades empresariales: En la mayoría de los casos, la operadora de drones trabaja para terceros. En consecuencia, deberá desarrollarse la correspondiente coordinación de actividades empresariales (art. 24 de la LPRL) que, en el caso de los vuelos de drone, pueden afectar tanto a la operadora y a su cliente como a terceros trabajadores que estén situados en la zona de vuelo.

Cuando los drones son utilizados en la construcción, se deberá tener en cuenta este aspecto en el Plan de Seguridad y Salud[9].

i) Riesgo grave e inminente. Se deberán definir las condiciones que pudieran sobrevenir durante el vuelo (climatológicas, agrupación de personas, presencia de otras aeronaves, etc.) que impidan el vuelo del dron en condiciones seguras tanto para el drone, el piloto y observadores como para las personas que se encuentren dentro de la zona de vuelo, debiendo éstas ser conocidas por el piloto.

j) Riesgo para terceras personas. El principal riesgo para terceras personas es el contacto con el dron, bien por caída o por contacto de proximidad. Este contacto puede ser directo y provocar daños sobre las personas, equipos e instalaciones y, en particular, sobre otras aeronaves dentro del espacio aéreo. Estos riesgos deberán ser controlados a través del cumplimiento de los requisitos de navegación aérea fijados por la legislación, pero además hay que tener en cuenta todo lo relacionado con la coordinación de actividades empresariales indicado en el art. 24 de la LPRL.

Pese a todo esto los drones se enfrentan a una serie de retos que deberán solventar, con el objetivo de integrase de forma segura en todos los ámbitos de la sociedad, también en las empresas. Se puede destacar los tres siguientes entre los muchos desafíos de los drones:

1. Utilizar el espacio aéreo abierto de manera integrada con el resto de las aeronaves.
2. Volar de manera interconectada con otros drones, transfiriéndose datos mutuamente, utilizando otras tecnologías como la IA para optimizar su actividad.

[9] Real Decreto 1627/1997, de 24 de octubre, por el que se establecen disposiciones mínimas de seguridad y de salud en las obras de construcción.

3. La privacidad y protección de los datos obtenidos con cámaras de video, fotos etc.

Finalmente, los drones pueden constituir una nueva herramienta tecnológica que facilite la realización de tareas para los trabajadores permitiendo trabajos más seguros y un mayor nivel de control, mejorando, consecuentemente, la PRL de las empresas.

3. Aparatos de Simulación (Realidad Virtual y Aumentada)

La realidad virtual y aumentada suelen ser la puerta de entrada de las empresas para introducirse en la Industria 4.0. Ambas utilizan elementos virtuales, una crea escenarios virtuales inmersivos (realidad virtual) y la otra incorpora elementos virtuales al mundo real (realidad aumentada), aportando información extra de utilidad.

Se define la realidad virtual[10] (RV), como el entorno digital y tridimensional generado por ordenador, u otros sistemas informáticos, en el que provoque en una persona una sensación de inmersión en un escenario aparentemente real, pudiendo interactuar con sus elementos.

Entre los objetivos de esta tecnología de RV se destacan:

- Generar un entorno lo más fiel posible a una realidad física determinada, "sustituyéndola".
- Construir un entorno irreal pero posible, en el que se elimina la frontera entre lo real e irreal y se difuminan los límites que separan ambos mundos.

La tecnología de RV es polivalente y con ello tiene multitud de aplicaciones. Como ejemplos que se pueden destacar, citaremos los usos más frecuentes, que van desde el entrenamiento de pilotos, astronautas o soldados, aplicaciones en la medicina educativa simulando operaciones, tratamiento de fobias contra insectos, a volar o a espacios pequeños, hasta la creación de entornos virtuales en museos, tiendas o aulas, además de estar presente en el ámbito del entretenimiento en multitud de juegos o cines 3D.

Por otro lado, la realidad aumentada (RA) viene ganando terreno en varios sectores debido a sus inúmeras utilidades. La tecnología RA es creada por un dispositivo que añade información adicional en tiempo real a una pantalla, a través de la cual la

[10] 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

persona observa el mundo físico; y como resultado visualiza una realidad enriquecida. Como consecuencia, puede incorporar información muy variada al mundo real. Según Ronald Azuma (1997), la RA debe cumplir tres requisitos:

- Combinar elementos virtuales y reales.
- Permitir interactividad en tiempo real.
- Almacenar información en 3D.

A un nivel más extendido, la RA tiene aplicaciones en sectores como el turismo, por ejemplo, al observar un paisaje se informa de lugares que visitar y distancia a los mismos o en la educación, que al visualizar un cuadro o escultura en un museo se obtiene información en pantalla sobre el autor, fecha, estilo, etc.

Habiendo definido y expuesto las principales características de estas dos tecnologías, se puede concluir que la diferencia principal entre la RV y la RA es que en la primera el mundo físico "deja de existir" al generarse un entorno digital que proporciona sensación total de realidad; mientras que en la segunda el mundo real sigue presente y es enriquecido incorporando información digital adicional.

Teniendo en cuenta el uso industrial de estas tecnologías, la Guía de Realidad Virtual y Realidad Aumentada del Proyecto R-Evolución Industrial también destaca las siguientes aplicaciones:

- La RV puede crear una simulación casi real del futuro producto, con todas sus características y permite probar diferentes acabados sin inversiones en la creación de prototipos físicos. Se utiliza como herramienta para la formación práctica del personal mediante la simulación de experiencias. Es una solución omnicanal con la que se establece una nueva relación con los clientes, a los que puede trasladar a un entorno virtual de fábrica. Es especialmente utilizada por los fabricantes y proveedores de maquinaria industrial y herramientas para mostrar sus productos a tamaño real sin estar en la planta.
- La RA permite el diseño y adecuación de instalaciones antes de su propio montaje. Consiste en proyectar una imagen a tamaño real de la máquina que se va a instalar en el espacio deseado, de forma que el personal técnico-montador puede valorar si la futura instalación es acorde al espacio y características técnicas de su propia fabrica o la del cliente. Además, facilita el control de las instalaciones proyectando

datos de eficiencia y productividad en tiempo real de cada proceso productivo, lo que permite al personal controlar el comportamiento de una planta, interactuar con sus diferentes elementos y favorecer la toma de decisiones para mejorar el funcionamiento completo de la fábrica. También se utiliza para la elaboración de catálogos virtuales. Se añade al catálogo una capa digital que permite visualizar a través de móviles o tablets los productos en 3D en el mundo real, pudiendo modificar sus atributos y visualizar sus despieces técnicos y procesos detallados.

En lo que se refiere a la PRL es evidente que estas tecnologías también pueden ser utilizada como elemento de apoyo. Se puede emplear en aspectos como:

- "La formación: mediante la simulación de situaciones reales de trabajo se mejora el aprendizaje. Los métodos prácticos permiten entender mejor y más rápido lo aprendido y retenerlo durante más tiempo.
- Aumento de la seguridad del personal. La RV elimina los riesgos del personal en formación cuando se abordan tareas que podrían comportar un riesgo para su integridad física o salud ya que en realidad no están expuestos, reduciendo la posibilidad de accidentes.
- Ante situaciones críticas o complejas, sitúa al personal en un entorno simulado parecido al real donde tienen que actuar como lo harían en su lugar de trabajo. Esto les ayuda a adquirir correctos hábitos de comportamiento ante una situación de riesgo real.
- La RA les ayuda en situaciones de riesgo, guiándoles para enfrentarse al peligro en momentos de estrés que podrían perturbar su correcta actuación. En caso de averías, les guía en su resolución, tengan o no formación, disminuyendo la exposición al riesgo al ser corregido en menos tiempo"[11].

Así como las anteriores tecnologías, la RV y RA tienen desafíos de cara a su futuro cercano para la efectiva implantación en el entorno laboral. Según la consultora Willis Towers Watson, actualmente "los acuerdos con los usuarios son insuficientes para cubrir

[11] 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

todas las posibilidades de uso indebido de una plataforma virtual y están lejos de dejar claro dónde recae la responsabilidad"[12].

Esto genera un gran problema si tenemos en consideración que la RV y RA tratan datos privados, transacciones y pagos reales, por lo que es necesario adaptar la normativa con respecto al desarrollo de estas tecnologías, al igual que los seguros individuales, corporativos y gubernamentales que debido a los avances van quedando obsoletos y resultan ineficaces en relación con la asignación de responsabilidades.

4. Equipos de Protección Individual con Sistemas de IoT

El sistema de "IoT" o del inglés *Internet of Things*, que traducido se refiere a la Internet de las Cosas, se trata de una red de objetos interconectados, "que se comunican entre sí, se transmiten información, se coordinan, identifican e interactúan entre ellas y los ordenadores"[13].

El proceso de conexión de un sistema mediante el Internet de las cosas comienza con la captación de datos que se derivan físicamente de los sensores. Luego comienza la comunicación y se envía a una plataforma de software que centraliza todos los datos recopilados (esta es la etapa en la que el mundo físico de las "cosas" se ha trasladado al mundo de las comunicaciones informáticas). Posteriormente, se procesan los datos y se procede a su explotación (esta etapa incluye el análisis y definición de ciertos modelos que permiten el aprendizaje por algoritmos). En última instancia, el objetivo es crear protocolos y procedimientos mejorados para la organización.

La digitalización y su introducción en las empresas va a aportar avances y mejoras en la prevención de accidentes. Una gran oportunidad de mejorar la gestión preventiva de las empresas con una efectiva orientación de las acciones en PRL así como para predecir posibles accidentes y favorecer su reducción.

Los conocidos como Smart EPI tienen esta finalidad, se tratan de equipos de protección individual inteligentes que, "ofrecen un mayor nivel de protección y más

---

[12] WTW, *Realidad virtual, aumentada y mixta: la cadena del riesgo se vuelve más compleja*, disponible en https://willistowerswatsonupdate.es/ciberseguridad/realidad-virtual-aumentada-mixta-riesgos/

[13] NAVAS NAVARRO, S. "Smart robots y otras máquinas inteligentes en nuestra vida cotidiana" en *Revista CESCO de Derecho de Consumo*, N.º 20/2016, disponible en https://revista.uclm.es/index.php/cesco/article/view/1249/1028

comodidad gracias al uso de materiales mejorados o componentes electrónicos"[14], además de la recogida y monitorización de datos, también ajusta el nivel de protección de las personas calibrándolo a los parámetros medidos. Un ejemplo es una chaqueta anticaída que se engancha a un cinturón y se infla automáticamente para mitigar el impacto de una caída cuando detecta que ambos pies no están en el suelo y tiene un estimulador de frecuencia cardíaca.

Las soluciones tecnológicas más extendidas referentes a los Smart EPI en el ámbito de la prevención laboral en las empresas son los equipos con incorporación sensórica embebida, que diferencia de las computadoras de propósito general, que están diseñadas para satisfacer una variedad de necesidades, los sistemas embebidos están diseñados para satisfacer necesidades específicas, y los sistemas IoT. A continuación, se diferencian dos tipos de sistemas IoT en EPI:

- Etiquetas en los EPI (Tags). Se trata de Códigos QR, Códigos de Barras, RFID (Radiofrecuencia), etc. que se añaden a los equipos de protección individual que utiliza el personal.
- EPI con sistemas IoT integrados en origen desde el diseño. Se trata de nuevos dispositivos que incluyen sensores integrados en el propio EPI para aumentar su utilidad y capacidad de proteger al usuario mediante el seguimiento de los datos que recopila. Estos son dispositivos son homologados.

Existen muchos ejemplos de Smart EPI con ambas tecnologías, desde cascos con detección de gas o sensores de posicionamiento, hasta dispositivos de protección auditiva que miden la intensidad del ruido, gafas con medidores de UV y más. Además, pueden emitir una alerta si se supera un determinado límite.

Entre los objetivos de implementar sistemas IoT en EPI, podemos destacar la agilidad en la gestión de EPI. Esta tecnología brinda información digital sobre los EPI y permite su trazabilidad, de esta manera se puede conocer las características de cada EPI, hacer seguimiento a la adquisición, compra y posterior entrega a los usuarios, además de controlar el mantenimiento y sus tiempos, el stock y seguir la caducidad y retirada.

[14] EU-OSHA, "Equipos de protección individual inteligentes: protección inteligente de cara al futuro" julio de 2020, disponible en https://osha.europa.eu/es/publications/smart-personal-protective-equipment-intelligent-protection-future

Además de automatizar el seguimiento del uso de EPI, evaluar la verdadera eficacia de los EPI o mejorar las investigaciones de accidentes.

El IoT es una oportunidad para que las empresas mejoren su desempeño en PRL mediante nuevas prácticas basadas en medir y "monitorizar" gran cantidad de parámetros de utilidad para PRL en continuo. Una adecuada gestión de la información según la secuencia "medir-registrar-analizar-actuar-revisar", permite tanto generar procesos de actuación inmediata (identificación de situaciones peligrosas, emisión de avisos y alertas, activación o inhibición de equipos o procesos, etc.), como analizar colectivamente un gran volumen de datos para ayudar en la toma de decisiones incluso en la prevención predictiva.

Entre los principales desafíos de esta tecnología estará establecer la finalidad de dicha tecnología y acotar la recogida de datos a este objetivo, teniendo en cuenta aspectos como la intimidad y privacidad de los trabajadores. Se debe establecer protocolos que garanticen la protección de los datos, buscando siempre el amparo de los criterios legales que marca la normativa.

Por otro lado, al introducir la electrónica en los EPI lo que fabricantes y organismos de evaluación de conformidad con arreglo al Reglamento relativo a los EPI de la UE[15] se enfrentan al reto de "aprender electrónica", realizando pruebas correspondientes de los EPI habituales, así como las relacionadas con la seguridad electrónica, seguridad de la batería, impacto electromagnético etc. Todavía no se dispone de una normativa específica para los EPI inteligentes[16], lo que provoca que no se tenga un criterio para evaluar la calidad de estos.

5. Software de Gestión

La gestión de los trabajadores basada en la IA (abreviatura del inglés AIWM) hace referencia a un sistema de gestión de los trabajadores que recopila datos, habitualmente en tiempo real, sobre el espacio de trabajo, los trabajadores, el trabajo que realizan y las herramientas digitales que utilizan para su trabajo, que luego se introduce en un modelo

[15] 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.

[16] Sin embargo, la CEN ha publicado una *guía en la que se recoge información y recomendaciones sobre textiles inteligente*s: CEN/TR 16298:2011, "Textiles inteligentes. Definiciones, categorización, aplicaciones y necesidades relativas a la normalización".

basado en la IA que toma decisiones automatizadas o semiautomatizadas o proporciona información a los responsables de la toma de decisiones sobre cuestiones relacionadas con la gestión de los trabajadores[17].

Según informe elaborado por la Agencia Europea para la Seguridad y la Salud en el Trabajo (EU-OSHA), la gestión de los trabajadores basada en la IA puede ofrecer posibles oportunidades para mejorar la SST de los trabajadores, por ejemplo, proporcionando herramientas para un mejor seguimiento de los riesgos y de la salud mental de los trabajadores, mejorando el compromiso y la satisfacción laboral de los trabajadores, ayudando a diseñar y llevar a cabo la formación en materia de seguridad, etc.

Sin embargo, los resultados indican que el uso de la IA para gestionar a los trabajadores también plantea numerosos riesgos para la SST, entre los que se incluyen, entre otros, la pérdida de control de los trabajadores sobre sus puestos de trabajo, el aumento de la intensidad del trabajo y de la presión sobre el rendimiento, la disminución del apoyo social de los directivos y la individualización y deshumanización de los trabajadores, la creación de un entorno competitivo poco saludable, la falta de transparencia y la pérdida de poder de los trabajadores y sus representantes, la desconfianza, la participación limitada de los trabajadores, el desequilibrio entre el trabajo y la vida privada, etc. Estos riesgos, a su vez, podrían tener numerosas consecuencias negativas para el bienestar físico y psicosocial de los trabajadores, como trastornos musculoesqueléticos (TME), trastornos cardiovasculares, fatiga, estrés, ansiedad y agotamiento.

El informe sugiere que es necesario un enfoque sólido de "prevención a través del diseño" que integre un enfoque centrado en el ser humano en el diseño y el uso de AIWM. La AIWM debe diseñarse, aplicarse y gestionarse de forma fiable, transparente, empoderadora y comprensible, garantizando la consulta, la participación y la igualdad de acceso a la información de los trabajadores, así como poniendo a los seres humanos en control y, por tanto, asegurando que la AIWM se utilice no para sustituir a los trabajadores, sino para apoyarlos.

---

[17] EU-OSHA, "Artificial intelligence for worker management: implications for occupational safety and health - Executive Summary", https://osha.europa.eu/es/publications/summary-artificial-intelligence-worker-management-implications-occupational-safety-and-health

Lo cierto es que la implantación de la AIWM debe estar, preferentemente, consensuada entre la empresa y los representantes de los trabajadores, con unos objetivos marcados por ambos y los datos obtenidos, procesados y analizados solo deben ser utilizados para cumplir dichos objetivos. En consecuencia, cualquier otro uso sería una utilización de datos que puede vulnerar la privacidad de los trabajadores, además de provocar todos los riesgos mencionados para la SST.

III. PRIMERAS RESPUESTAS NORMATIVAS DE LA UE EN MATERIA DE SEGURIDAD Y RESPONSABILIDAD CIVIL

1. Aproximación a los Retos que Plantea la Incorporación de los Sistemas de IA en el Ámbito Laboral.

Vistas algunas de las tecnologías disruptivas que incorporan los sistemas de IA, se puede reflexionar sobre los retos que plantea su fabricación, comercialización y aplicación en la UE. En la raíz de estos retos se encuentran:

- Heterogeneidad de las tecnologías: la gran cantidad de soluciones tecnologías de tan diferentes características hace con que la normalización sea más difícil que la de otros productos y servicios.
- Sometimiento a constantes actualizaciones (mediante internet o no): la IA es una tecnología habilitadora que está sujeta a cambios extremadamente rápidos de investigación y desarrollo, lo que hace que las normas técnicas puedan quedar obsoletas muy rápidamente. De ahí que las normas se enfrenten al reto de tener que ser actualizadas o reformuladas en un plazo relativamente corto.
- Actualizaciones realizadas por distintos operadores: Hay cada vez más operadores que intervienen en la cadena de valor del producto, dejamos atrás la etapa de que un fabricante produce el bien y el empresario lo compra, para pasar a un fabricante, a un empresario que actualiza y que lo usa, distintos fabricantes del producto físico y del sistema de inteligencia artificial etc.
- Seguridad y privacidad: dejamos atrás el concepto clásico de seguridad, entendido como una máquina que genera unos riesgos (atrapamiento, ruido etc.), sino que pasamos a un robot con IA que puede estar recogiendo datos constantemente de trabajadores, afectando a su privacidad. Por ello

es necesario saber si se pueden utilizar dicha información y en caso de que se pueda establecer para que fines.

- Complejidad e interconectividad: Muchos sistemas de IA constan de una multiplicidad de componentes y procesos diferentes que están interconectados. Esta complejidad e interconectividad dificulta el control, la identificación y la prueba de posibles infracciones de las leyes.
- Comportamiento autónomo: La capacidad de algunos sistemas de IA para generar resultados con una intervención humana limitada o nula puede violar las normas de seguridad y los derechos humanos que pueden pasar desapercibidos.
- Opacidad: La falta de transparencia de los sistemas de IA dificulta el control, la identificación y la prueba de posibles infracciones de las leyes, incluidas las disposiciones legales que protegen los derechos fundamentales de los seres humanos.

Teniendo en cuenta este horizonte de desafíos que florecen con los sistemas de IA, se realizará a continuación un análisis de las actuaciones de la UE para solventar la problemática planteada y establecer un nuevo marco jurídico para esta tecnología.

2. La Adaptación de la Normativa de Seguridad del Producto

2.1. Marco normativo existente

La tecnología progresando rápidamente en aspectos técnicos del diseño y fabricación contrasta con la lentitud en relación con la problemática jurídica, ética y de seguridad, consecuentemente también de PRL, decurrente de la aplicación de los robots inteligentes en las empresas. La preocupación por la seguridad ligada a la robótica no es nueva, y conforme la tecnología progresa también hay una exigencia normativa mayor referente a su diseño y fabricación.

Para situar el marco jurídico actual se debe partir de la Directiva 2006/42/CE del Parlamento Europeo y el Consejo, de 17 mayo relativa a las máquinas. Normativa traspuesta a través del RD 1644/2008, de 10 de octubre, por el que se establecen las normas para la comercialización y puesta en servicio de las máquinas.

El objetivo principal de estas disposiciones es eliminar las barreras a la libre circulación de máquinas en la Unión Europea, como refiere la propia Directiva, mediante

la armonización de los requisitos esenciales de seguridad y salud aplicables a su diseño y construcción que garanticen un nivel elevado de seguridad. La Directiva de Máquinas se aplica a la primera comercialización y/o puesta en servicio en la Unión Europea, es decir, a las maquinas nuevas fabricadas en la Unión Europea y a las nuevas y/o usadas procedentes de terceros países.

Por lo tanto, esta Directiva de Máquina 2006/42/CE y, por ende, el RD 1644/2008 están direccionadas a los fabricantes, que deben probar que han adoptado las medidas adecuadas para garantizar la seguridad de su máquina. Más específicamente, deben:

- Asegurar que la máquina cumple con los requisitos esenciales de seguridad y salud que figuran en la Directiva.
- Poner a disposición el expediente técnico referenciado en los anexos de la Directiva.
- Facilitar las informaciones necesarias, por ejemplo, las instrucciones.
- Llevar a cabo el procedimiento de evaluación de conformidad.
- Redactar la declaración CE de conformidad, adjuntándola a la máquina.
- Colocar el marcado CE.

Cumplidos los requisitos estipulados en la Directiva para comercialización y puesta en servicio de una máquina, se presume que el producto es seguro y pueden circular libremente en la UE.

En este sentido es importante saber la definición de fabricante, el RD especifica que es la "persona (física o jurídica) que diseña y/o fabrica una máquina o una cuasi máquina cubierta por la Directiva y que sea responsable de la conformidad de dicha maquina con vistas a su comercialización…"[18]. Sin embargo, también será considerado fabricante quien cambia el uso previsto de la máquina, recayendo en él la responsabilidad de las consecuencias que se deriven de las modificaciones efectuadas o quien ensambla máquinas, partes de máquinas o cuasi máquinas de orígenes diferentes para crear un conjunto y otra máquina.

[18] Artículo 2 apartado i) de la DIRECTIVA 2006/42/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de mayo de 2006 relativa a las maquinas y por la que se modifica la Directiva 95/16/CE.

En la práctica se puede tener diferentes casuísticas para establecer el fabricante de una máquina, por ejemplo:

1. En el caso de considerar que una empresa X solicita a otra empresa Y, de ingeniería, el diseño de una máquina y la fabricación de esta, la empresa Y sería la fabricante.
2. En este mismo caso, si la empresa Y realiza el diseño, pero a su vez manda a la empresa Z realizar la parte física del proceso, partiendo de un expediente técnico ya elaborado, también se considera fabricante a la empresa Y.
3. En la situación de que la empresa X compre diferentes máquinas de distintos fabricantes (Y, Z) y monta un conjunto de máquinas para funcionar como una sola, la empresa X se convierte en fabricante.
4. También será fabricante la empresa X si compra una máquina de la empresa Y pero realiza una modificación sustancia de la máquina por su cuenta.

Teniendo en claro los aspectos comentados sobre la normativa actual de comercialización y puesta en servicio de una máquina, ¿cómo se aplicaría en el caso de los equipos de trabajo con sistemas de IA? Es decir, cuando una máquina o robot incorpore un sistema de IA, que cada uno puede ser fabricado por distintas empresas, causando la intervención de más de un fabricante en el producto, cause un accidente ¿quiénes serán los sujetos responsables? Sin duda, este es uno de los nuevos retos que la normativa actual no es capaz de resolver y se hace necesaria la elaboración de un nuevo texto normativo centrado en las nuevas necesidades provocadas por el desarrollo de la tecnología con los sistemas de IA.

Según la actual normativa, como se ha visto, el responsable de cumplir los requisitos de la Directiva es el fabricante del producto. Sin embargo, cuando una máquina incorpora un sistema de IA, de otros fabricantes, que permite a la máquina actuar de manera autónoma, siendo capaz de aprender nuevos comportamientos (a partir de los datos almacenados), y formas interactuar con el entorno, que pueden provoca actuaciones impredecibles, es lógico pensar que el operador del sistema de IA debe tener responsabilidad y no únicamente el fabricante del producto físico.

Del mismo modo, según la normativa actual una vez que la máquina esta comercializada y puesta en servicio en una empresa, las obligaciones posventa del fabricante prácticamente son inexistente. La obligación de mantener la maquina en

condiciones de seguridad y salud en la empresa acaba recayendo sobre el empresario por medio de la aplicación del RD 1215/1997, de 18 de julio, por el que se establecen las disposiciones mínimas de seguridad y salud para la utilización por los trabajadores de los equipos de trabajo.

Este RD esta dirigido a los empresarios y establecen que ellos deberán adoptar las medidas necesarias para que los equipos de trabajo, incluido los robots, que se pongan a disposición de los trabajadores sean adecuados al trabajo que deba realizarse y convenientemente adaptados al mismo, de forma que garantice la seguridad y salud de los trabajadores al utilizar dichos equipos.

Según esta disposición, solo deben utilizarse equipos de trabajo que sean "seguros para el uso previsto". Este principio se tendrá en consideración a la hora de la elección de equipos que van a ponerse a disposición de los trabajadores, ya sean nuevos o usados. Así el empresario debe asegurarse de que, por diseño o por características constructivas, el equipo seleccionado es adecuado para el trabajo a realizar, considerando algunos aspectos como el producto a fabricar o proceso a desarrollar y las materias primas a utilizar, los objetivos de producción, el espacio disponible entre otros.

Sin embargo, estas disposiciones dejan huérfanos de solución los problemas que derivan del empleo industrial y colaborativo de los robots, y de la aplicación de los sistemas de IA. Los equipos con tecnología empleada en el "Internet de las Cosas" pueden interactuar entre sí, es decir, pueden compartir la información que han obtenido y llevar a los equipos que están interactuando a realizar acciones que no estaban previstas por el operador del sistema debido a la obtención de estos datos y esto provoque un accidente con daños.

Asimismo, como la gran mayoría de los equipos informáticos, los robots inteligentes y las demás tecnologías también necesitan de actualizaciones. Sin embargo, el marco normativo actual no es suficiente para establecer este compromiso porque no hay obligaciones posventa para los fabricantes. Es necesario crear normas para favorecer las actualizaciones en remoto y establecer requisitos de revisión y control por el fabricante sobre cualquier software de terceros que pudiera conectarse a los dispositivos de IoT.

En este sentido la UE viene trabajando en una nueva propuesta de Reglamento en materia de IA para atajar todas estas cuestiones planteadas, que con la normativa actual no quedan solventada. La conocida como Ley de Inteligencia Artificial (de aquí en

adelante, Ley de IA) establece los requisitos mínimos necesarios para subsanar los riesgos y problemas vinculados a la IA, sin obstaculizar ni impedir el desarrollo tecnológico y sin aumentar de un modo desproporcionado el coste de introducir soluciones de IA en el mercado.

A continuación, se tratará de realizar un análisis de dicha propuesta de reglamento para dar respuesta a todos los flecos abierto respecto a la IA y su implantación en el mundo laboral.

2.2. Ley de Inteligencia Artificial

Los nuevos retos jurídicos que propone el desarrollo de sistemas de IA deben afrontarse estableciendo la máxima seguridad jurídica en toda la cadena de responsabilidad, particularmente para el productor, el operador, la persona afectada y cualquier otro tercero. Se ha visto como la normativa actual es insuficiente para responder a estos desafíos relacionados con la seguridad frente a los daños producidos por productos que integren sistemas de IA.

En abril de 2021, la Comisión Europea presentó su propuesta de Reglamento por el que se establecen normas armonizadas sobre la IA[19], la llamada "Ley de Inteligencia Artificial". Por un lado, la propuesta tiene la pretensión de establecer un marco jurídico destinado a lograr que la IA cumpla con el derecho y los valores de la Unión. Por otro, se esta trabajando en la UE en una nueva normativa de seguridad de máquinas buscando actualizar la actual para mejorar, simplificar y adaptarla a las necesidades del mercado.

La propuesta se basa en un enfoque orientado al riesgo, esto quiere decir que no todos los sistemas de IA están sujetos a las mismas reglas[20]. Se aplica un enfoque de aplicación gradual en función del riesgo que genera los sistemas de IA. De este modo la Ley de IA regula cuatro categorías de riesgos, que son:

1. Riesgo inaceptable
2. Alto riesgo
3. Riesgo limitado

---

[19] EUROPEAN COMMISSION, "Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", COM(2021) 206 final.

[20] AISLINN, K. "The AI Act and algorithmic management", op. cit. p. 3, disponible en https://cllpj.law.illinois.edu/content/dispatches/2021/Dispatch-No.-39.pdf

4. Riesgo bajo o mínimo

Los sistemas de IA que supongan un "**riesgo inaceptable**" estarán prohibidos, por ser contrario a los valores de la Unión, como respeto a la dignidad humana, libertad, igualdad y afectar derechos fundamentales, debido a que sus prácticas tiene un gran potencial para manipular a las personas mediante técnicas subliminales que alteran al comportamiento de humano, transciendiendo su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad.

Igualmente se consideran como riesgo inaceptable, que las autoridades públicas lleven a cabo calificación social con base en la IA con fines generales o que se utilice sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo excepciones limitadas.

Sin embargo, la mayor parte de las disposiciones de la Ley de IA se refieren a los sistemas de "**alto riesgo**", que están permitidos en el mercado europeo, pero estableciendo obligaciones para los proveedores, usuarios y otros participantes en la cadena de valor de la IA. Estos sistemas están sujetos al cumplimiento de requisitos obligatorios y a una evaluación de conformidad "ex ante", antes de poder comercializarlos (art. 8 y ss. de la Ley de IA).

Los sistemas de IA de alto riesgo acarrean riesgos importantes para la seguridad y salud o los derechos fundamentales de las personas. Para considerarse como sistema de IA de alto riesgo se debe tener en cuenta su finalidad prevista, pero además la finalidad especifica y las modalidades para las que se use dicho sistema. La calificación de "Alto Riesgo" se define en las dos categorías principales de sistemas de IA (art. 6):

1. los sistemas de IA que son en sí mismos productos o bien componentes de seguridad de productos ya cubiertos por determinada legislación de armonización de la Unión en materia de salud y seguridad;
2. los sistemas de IA independientes o no incorporados a otros productos específicos; con implicaciones relacionadas con los derechos fundamentales, que aparecen especificados en el anexo III.

La aplicación potencial al trabajo de los sistemas de IA de alto riesgo se limita fundamentalmente al ámbito de la aplicación biométrica (que no se encuentra como

prohibido) y al del "empleo, gestión de los trabajadores y acceso al autoempleo" (segunda subcategoría, del Anexo III) distinguiéndose dentro del mismo los supuestos siguientes:

a) "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;
b) IA destinada a utilizarse para tomar decisiones relativas a la promoción y resolución de relaciones contractuales de índole laboral, a la asignación de tareas y al seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones"[21].

Por lo tanto, la consideración de un sistema de IA como de alto riesgo se reserva, para los sistemas de IA que se utilizan para "la contratación y la selección de personal, para la toma de decisiones relativas a la promoción y la rescisión de los contratos, y para la asignación de tareas y el seguimiento o la evaluación de personas en relaciones contractuales de índole laboral", y ello porque "pueden afectar de modo considerable a las futuras perspectivas laborales y los medios de subsistencia de dichas personas"[22].

"Dichos sistemas 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".

Con relación a los sistemas de IA con un "**riesgo limitado**", el título IV de la Ley de IA establece obligaciones de transparencia. Según la norma "los proveedores garantizarán 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"[23]. Basado en esta obligación, se entiende que los

[21] Anexo III.4, Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, de la Ley de IA.

[22] Considerando 36 de la Propuesta.

[23] Artículo 52 del la Ley de IA: Obligaciones de transparencia para determinados sistemas de IA.

sistemas de IA con un riesgo limitado son los que, no siendo de alto riesgo, están diseñados para interactuar con las personas.

Aparte de obligacion a los proveedores, también se especifica que los usuarios de estos sistemas de IA, que a su vez, incorpore "un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él". También informarán que un contenido ha sido generado de forma artificial o manipulado en caso de contenido de imágenes, sonidos o videos que puedan inducir erroneamente a una persona a pensar que son autenticos o verídicos (ultrafalsificación).

Por ultimo, son los sistemas de IA que provocan un "**riesgo mínimo**". Están incluidos en esta calificación todos aquellos sistemas de IA que pueden desarrollarse y utilizarse con arreglo a la legislación vigente sin obligaciones jurídicas adicionales. "El regulador considera que la mayoría de los sistemas de IA utilizados actualmente en la UE pertenecen a esta categoría. Y tan solo sugiere que, por parte de los proveedores, se opte voluntariamente por aplicar los requisitos de una IA digna de confianza y adherirse a códigos de conducta voluntaria con los requisitos establecidos para una IA de alto riesgo (art. 69)"[24].

Es importante que los sistemas de IA asociados a productos que el presente Reglamento no considera de alto riesgo y que, por lo tanto, no están obligados a cumplir los requisitos establecidos en él sean, no obstante, seguros una vez introducidos en el mercado o puestos en servicio. Para contribuir a este objetivo, se aplicaría, como red de seguridad, se está reformando la Directiva 2001/95/CE del Parlamento Europeo y del Consejo[25].

La propuesta de la Comisión Europea trata, en el art. 16 de la Ley de IA, de las obligaciones relacionadas con los sistemas de IA de alto riesgo. La mayoría de los requisitos mencionados se dirigen a los proveedores, es decir, a la persona u organismo

[24] GOÑI SEIN, J.L. "Ley de inteligencia artificial y seguridad y salud en el trabajo" 2022*, en prensa*.

[25] Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (DO L 11 de 15.1.2002, p. 4).

que desarrolla un sistema de IA o que hace desarrollar un sistema de IA con el fin de comercializarlo o ponerlo en servicio bajo su propio nombre o marca[26].

Se impone a los proveedores las siguientes obligaciones:

- Evaluación previa de la conformidad: Los proveedores deben garantizar que el sistema de IA de alto riesgo se somete a un procedimiento de evaluación de la conformidad ex ante, antes de que el sistema se comercialice o se ponga en servicio[27]. La evaluación se basa en verificaciones de control interno, para lo que se requiere una autoevaluación. Únicamente quedan exceptuados de la autoevaluación los sistemas de identificación biométrica remota que están sujetos a una evaluación de la conformidad realizada por un tercero[28] y otros sistemas que necesitan la participación de un organismo notificado independiente[29]. La evaluación de la conformidad les permitirá a los proveedores demostrar el cumplimiento de los requisitos obligatorios. Además, colocarán el marcado CE para indicar que cumplen lo dispuesto en el presente Reglamento[30].
- Sistema de gestión de la calidad: Los proveedores deben implantar un sistema de gestión de la calidad para la conformidad que incluya, sobre todo, procedimientos de examen, prueba y validación que se lleven a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo[31].
- Registro: Los proveedores deben registrar todos los sistemas autónomos de IA de alto riesgo en una base de datos de la UE, antes de comercializar el sistema o ponerlo en servicio[32]. La información contenida en la base de datos de la UE será accesible al público[33].

---

[26] Art. 3 de la Ley de IA

[27] Art. 19 de la Ley de IA,

[28] PONCE, A. "The AI Regulation: Entering an AI Regulatory Winter? Why An Ad Hoc Directive on Ai in Employment Is Required", *ETUI Research Paper* - Policy Brief 2021.07.7, Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873786

[29] Art. 43.1.b), Anexo VII de la Ley de IA.

[30] De conformidad con el artículo 49 de la Ley de IA.

[31] Art. 17.1.d) de la Ley de IA.

[32] Art. 16.f), 51, 60, Anexo VIII de la Ley de IA.

[33] Art. 60.3 Ley de IA.

- Seguimiento posterior a la comercialización: Los proveedores están obligados a establecer, aplicar y mantener un sistema de seguimiento posterior a la comercialización[34]. El sistema de seguimiento deberá recoger, documentar y analizar de forma activa y sistemática los datos pertinentes sobre el funcionamiento de los sistemas de IA de alto riesgo a lo largo de su vida útil, con el fin de permitir al proveedor evaluar el cumplimiento continuo de los sistemas de IA con los requisitos del reglamento[35]. En caso de que un proveedor tenga motivos para considerar que los sistemas de IA de alto riesgo no son conformes con el Ley de IA, el proveedor adoptará inmediatamente las medidas correctoras necesarias para que ese sistema sea conforme, retirándolo o recuperándolo, según proceda[36].
- Informar a las autoridades competentes: Si un sistema de IA de alto riesgo tiene el potencial de afectar negativamente a la salud, la seguridad o los derechos fundamentales, en un grado que va más allá de lo que se considera razonable y aceptable en relación con su finalidad prevista o en las condiciones normales o razonablemente previsibles de uso, y este riesgo es conocido por el proveedor, éste debe informar inmediatamente a las autoridades nacionales competentes, en particular de la no conformidad y de las medidas correctoras adoptadas[37].

Por otro lado, desde el ámbito de la PRL debe existir una conexión coherente entre la Ley de IA y la Directiva 89/391/CEE, Marco de seguridad y salud en el trabajo. Esto se traduce en que los sistemas de IA de alto riesgo no deben cumplir solamente con los riesgos específicos de la seguridad de IA, sino que también los de la seguridad general del producto final, incluyendo el propósito de seguridad y salud en el trabajo.

Sin embargo, lo que se entiende como riesgo para la Ley de IA no es lo mismo que para la Directiva, si tenemos en cuenta que las principales obligaciones que se regulan en la Ley esta destinada únicamente a los sistemas de IA que producen un alto riesgo, y para la Directiva se considera el concepto riesgo en su amplitud. El propio Considerando 27 de la Ley de IA dicta que "calificación 'de alto riesgo' debe limitarse a aquellos

[34] Art. 17.1.h), 61.1 de la Ley de IA.

[35] Art. 61.2 de la Ley de IA.

[36] Art. 16.g) y 21 de la Ley de IA.

[37] Art. 22, 65.1 de la Ley de IA en relación con el Art. 3 nº 19 del Reglamento 2019/1020.

sistemas de IA que tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación reduce al mínimo cualquier posible restricción del comercio internacional, si la hubiera". Por lo tanto, no son todos los sistemas que estarán sujetos a estas obligaciones de marcará el artículo 9 de la Ley de IA, sobre los Sistemas de gestión de riesgos, si no que debe existir consecuencias adversas del sistema para la seguridad que sean significativas.

En el lugar de trabajo, al aplicar los sistemas de IA se produce un efecto de doble sentido:

- En primer lugar, se excluyen todos los sistemas de IA que no representen un efecto grave o alto para los trabajadores. Aunque el sistema pueda generar un peligro para los trabajadores no será necesario cumplir con los requisitos esenciales de alto riesgo, y simplemente se exigirán obligaciones específicas de trasparencia de los riesgos limitados o mínimos.
- En segundo lugar, en gran medida los sistemas de IA considerados de alto riesgo en el trabajo, producen "efectos apreciables de impacto negativo en la seguridad de las personas son de carácter psicológico… pero ello se va generando paulatinamente y *a priori* podría no ser considerado de alto riesgo, a la luz de la Ley de IA, por no suponer un fuerte impacto"[38] debido a que el impacto nocivo no aparece inmediatamente si no que es un proceso gradual'[39]

En lo que se refiere a las obligaciones del usuario o empleador, este tiene las mismas obligaciones que las estipuladas por la LPRL, como, por ejemplo, eliminar o reducir los riesgos. Sin embargo, la Ley de IA estipula un sistema de gestión de riesgo, que según su art. 9.2 se pueden distinguir tres etapas, que son:

[38] GOÑI SEIN, J.L. "Ley de inteligencia artificial y seguridad y salud en el trabajo" 2022, P.19, *en prensa*.

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

1. "Identificación y el análisis de los riesgos conocidos y previsibles vinculados a cada sistema de IA de alto riesgo".
2. Evaluación de los riesgos, de la siguiente manera:
    a. "la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo en cuestión se utilice conforme a su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible".
    b. "la evaluación de otros riesgos que podrían surgir a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización[40]…".

    "En esa evaluación de riesgos potenciales de la IA, el proveedor deberá tener en cuenta, cuando el sistema de IA se integre en el trabajo, la concreta finalidad para la que está prevista; y analizar de qué modo el sistema de IA afecta a la seguridad y salud de los trabajadores. Pero, además, deberá evaluar los riesgos derivados de un uso indebido razonablemente previsible, lo que, tratándose del contexto laboral, supone contemplar los posibles usos desviados o ilícitos del sistema de IA que pueda hacer el usuario/empresario; es decir, los diseñados con un propósito y, una vez implementados, utilizados con otro fin"[41].
3. "Adopción de medidas oportunas de gestión de riesgos": Según los criterios marcados en el Art. 9.4, que son:
    a. "eliminar o reducir los riesgos en la medida en que sea posible mediante un diseño y un desarrollo adecuados;
    b. implantar, cuando proceda, unas medidas de mitigación y control apropiadas en relación con los riesgos que no puedan eliminarse;
    c. proporcionar la información oportuna conforme al artículo 13, en particular en relación con los riesgos mencionados en el apartado 2, letra b), del presente artículo y, cuando proceda, impartir formación a los usuarios".

Los proveedores no tienen la obligación de eliminar el riesgo, lo que se espera de ellos es que lo identifiquen, lo reduzcan, lo controlen y que proporcionen información al

[40] Referente al Art. 61 de la Ley de IA.

[41] GOÑI SEIN, J.L. "Ley de inteligencia artificial y seguridad y salud en el trabajo" 2022, P.20*, en prensa*.

respecto. En este sentido, los riesgos residuales se consideran "aceptables" siempre que las medidas de gestión de riesgos sean suficientes y el sistema de IA se utilice de acuerdo con su finalidad prevista o en condiciones de "uso indebido razonablemente previsible". La única obligación es que esos riesgos residuales tienen que ser comunicados[42].

Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de un modo adecuado para su finalidad prevista y cumplen los requisitos establecidos en el presente capítulo 2 de la Ley de IA.

Por ultimo, en referencia a la documentación técnica de los sistemas de alto riesgo, esta "se preparará antes de su introducción en el mercado o puesta en servicio, y se mantendrá actualizada", conforme la información del anexo IV.

2.3. Máquinas/IA

El avance de la tecnología de los sistemas de IA no solo tiene repercusiones por el establecimiento de una nueva normativa, que permite instaurar un nuevo marco jurídico, si no que también conlleva a revaluar aquellas normativas que pueden trabajar en sinergia para lograr el objetivo de la seguridad y salud, y la protección de los derechos fundamentales. Lo cierto es que las máquinas también están evolucionando y muchas de ellas ya están incorporando sistemas de IA para realizar sus funciones. Esto se traduce en una interrelación entre las dos normativas, IA y máquinas.

La complementariedad entre las propuestas legislativas relativas a la IA artificial y a las máquinas simplifica las cargas de los fabricantes ya que el Reglamento sobre la IA delega la evaluación de conformidad en las máquinas, de modo que la evaluación de riesgos de las máquinas completas con sistemas de IA solo se llevará a cabo a través del futuro Reglamento relativo a las máquinas y sus partes y accesorios, pero deberán aplicar lo especifico de la Ley de IA que afecte a su producto.

En lo referente a la revisión de la Directiva de Máquinas 2006/42/CE, se trata de la principal normativa de la UE para empresas que diseñen, fabriquen y distribuyan

[42] PONCE, A. "The AI Regulation: Entering an AI Regulatory Winter? Why An Ad Hoc Directive on Ai in Employment Is Required", *ETUI Research Paper* - Policy Brief 2021.07 9. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873786

máquinas porque contiene los requisitos esenciales de seguridad. Ante la vertiginosa evolución de la tecnología y por los cambios que ha sufrido la industria se ha quedado obsoleta en algunas cuestiones. Por ello, es inevitable que se plantee la revisión de dicha normativa para establecer un nuevo reglamento de máquinas en la UE. De hecho, la Comisión Europea ha elaborado un borrador sobre un nuevo Reglamento sobre Seguridad en Máquinas[43]

Entre las limitaciones que presenta la actual directiva de máquinas en relación con los sistemas de IA se encuentra la insuficiencia de la normativa ante los riesgos asociados a las nuevas tecnologías emergentes, especialmente la IA. Además de incoherencias con respecto a la nueva normativa europea de IA. Esto provoca una inseguridad jurídica respecto a posibles daños causados por estas nuevas tecnologías y, en consecuencia, la responsabilidad de los fabricantes y operadores.

El Nuevo Marco Legislativo se caracteriza por una legislación sobre la seguridad de los productos que especifica únicamente los requisitos esenciales que deben cumplir los productos comercializados en la UE para poder disfrutar de la libre circulación en el mercado interior, mientras que la tarea de dar una forma más concreta a estos requisitos esenciales, que se podrán en práctica por medio de normas técnicas armonizadas, se confía a las tres organizaciones europeas de normalización (OEN): CEN, CENELEC y ETSI. Este Nuevo Marco, en cuanto a las especificaciones técnicas, admitirá también una presunción de conformidad en caso de cumplimiento total o parcial de las normas técnicas armonizadas. La propuesta para los sistemas IA también tiene en cuenta la situación una vez que los sistemas de IA se han introducido en el mercado, pues armoniza la manera en que se llevan a cabo los controles ex post.

Una de las principales modificaciones del Reglamento de máquinas es la inclusión de los sistemas de IA que garantizan las funciones de seguridad o los software que garantiza las funciones de seguridad, incluidos los sistemas de IA, en el anexo I de máquinas y sus partes y accesorios de alto riesgo. Esto supone que estas máquinas de alto riesgo, con la nueva normativa, deberán pasar obligatoriamente por la certificación de un Organismo Notificado (ON), lo que actualmente no ocurre porque tienen la posibilidad

[43] Propuesta del Parlamento Europeo y del Consejo relativo a las máquinas y sus partes y accesorios (2021/0105 (COD).

de elegir si certificar mediante un ON o la autocertificación del fabricante si este había aplicado las normas armonizadas pertinentes[44].

El reglamento también ampliará la definición relativa a la "modificación sustancial" de la máquina, así como las consecuencias legales asociadas. Se integra en la definición las modificaciones por medios físicos o digitales no previstas por el fabricante y debido a la cual pueda verse afectada la conformidad del producto con los requisitos esenciales de salud y seguridad. El objetivo de esta modificación es garantizar que las máquinas introducidas en el mercado o puestas en servicio que sufran modificaciones sustanciales cumplan los requisitos esenciales de salud y seguridad del anexo III.

Otra de las modificaciones respecto de la Directiva vigente, es que se autorizará la entrega digital de las instrucciones de uso de las máquinas; aunque, a petición del cliente, el fabricante las proporcionará impresas.

3. La Adaptación de la Normativa de Responsabilidad Civil

3.1. Marco normativo existente

Los nuevos retos jurídicos que propone el desarrollo de sistemas de IA deben afrontarse estableciendo la máxima seguridad jurídica en toda la cadena de responsabilidad, particularmente para el productor, el operador, la persona afectada y cualquier otro tercero. Lo cierto es que la normativa actual no responde a varias cuestiones dejando varios flecos sin regulación. Se llevará a cabo un análisis a continuación para determinar las carencias actuales de dicha legislación y cómo la Unión Europea está buscando solucionar estos problemas actuales en materia de responsabilidad.

La Directiva 85/374/CE de responsabilidad por los daños causados por Productos defectuosos, es el marco europeo con respecto a la responsabilidad de los fabricantes ante los daños causados por los productos defectuosos. Dicha Directiva fue traspuesta al ordenamiento español en la Ley 22/1994 de 6 de julio, de responsabilidad civil por los daños causados por productos defectuosos, que actualmente se encuentra vigente por medio del RD 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la

[44] Artículo 12.3.1 de la 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

Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (LGDCU).

Lo primero que se debe tener claro es que la Directiva considera que un producto es defectuoso cuando el producto no ofrezca la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y, especialmente, su presentación, el uso razonablemente previsible del mismo y el momento de su puesta en circulación. Por otro lado, la Directiva del Consejo, 2001/95/CE de 3 de diciembre de 2001, relativa a la seguridad general de los productos, en su artículo 2.b) define lo que se entiende por producto seguro "cualquier producto que, en condiciones de utilización normales o razonablemente previsibles, incluidas las condiciones de duración y, si procede, de puesta en servicio, instalación y de mantenimiento, no presente riesgo alguno o únicamente riesgos mínimos, compatibles con el uso del producto y considerados admisibles dentro del respeto de un nivel elevado de protección de la salud y de la seguridad de las personas(…)"[45]

La Directiva 85/374/CE obliga a responder del daño al productor, definiéndolo como la persona que fabrica el producto terminado. De mismo modo se considera responsable a quién produce únicamente la materia prima o las partes que integrantes el producto, poniendo su nombre, marca o signo distinto en el producto. También al importado e incluso al suministrador se le puede considerar responsable si el productor no puede ser identificado dentro de un plazo razonable.

Esta Directiva establece una responsabilidad objetiva por productos defectuosos, que está concebida como una responsabilidad objetiva no absoluta u objetiva matizada, esto es, no se responde por la simple causación del daño, sino que el perjudicado debe

[45] (…) habida cuenta, en particular, de los siguientes elementos:

i) características del producto, entre ellas su composición, envase, instrucciones de montaje y, si procede, instalación y mantenimiento.

ii) efecto sobre otros productos cuando razonablemente se pueda prever la utilización del primero junto con los segundos,

iii) presentación del producto, etiquetado, posibles avisos e instrucciones de uso y eliminación, así como cualquier otra indicación o información relativa al producto,

iv) categorías de consumidores que estén en condiciones de riesgo en la utilización del producto, en particular los niños y las personas mayores. La posibilidad de obtener niveles superiores de seguridad o de obtener otros productos que presenten menor grado de riesgo no será razón suficiente para considerar que un producto es peligroso".

probar el defecto del producto, el daño producido y la relación de causalidad entre ambos. Sin embargo, se permite al productor exonerarse de responsabilidad en determinados supuestos de inimputabilidad, como si prueban la no puesta en circulación del producto, la inexistencia del defecto en el momento de la puesta en circulación, la producción con un destino no comercial, la elaboración conforme a normas imperativas existentes etc.

Además, la responsabilidad del productor se reduce si el daño es causado por una combinación de defectos del producto y culpa de la parte perjudicada. Con respecto al damnificado, esta responsabilidad del productor no puede ser limitada o excluida, y cualquier disposición en este sentido es nula. Por fin, una vez establecida la responsabilidad, si hubiera varias personas responsables, lo serán todos de forma solidaria.

Uno de los múltiples problemas que se plantean es el relativo a esta responsabilidad civil por los daños que puedan causar los dispositivos o máquinas basados en IA. Las soluciones previstas en los sistemas europeos tradicionales de responsabilidad civil extracontractual y en la legislación específica sobre productos defectuosos no parecen ajustarse bien a las características de esta nueva tecnología.

Las dificultades principales provienen de que estas máquinas, al contrario de lo que ocurre con cualquier otro tipo de tecnología hasta ahora conocida, se caracterizarían por su alto grado de "autonomía", su capacidad de "autoaprendizaje" y la posibilidad de que adopten "decisiones" no programadas y, por tanto, no previsibles de antemano.

Podrían darse situaciones en las que el dispositivo o máquina pudiera llevar a cabo acciones no previstas por el fabricante, el propietario o el usuario y que tales acciones causaran daños a terceros. En esos casos, en la producción del daño podría no concurrir ningún elemento de "culpa o negligencia" directamente atribuible a ninguna persona física ni jurídica y, por tanto, podría no ser exigible responsabilidad con arreglo a las normas generales de responsabilidad extracontractual. Y podría no existir tampoco propiamente ningún "defecto" en el diseño y fabricación del dispositivo o máquina, como requiere actualmente la normativa sobre productos defectuosos.

Además, incluso si existiera algún grado de negligencia en la producción o la utilización de la máquina, o algún elemento defectuoso en su diseño o fabricación, la propia complejidad del dispositivo y de los algoritmos y elementos técnicos empleados en su producción -elementos que, además, pueden provenir de distintos fabricantes y

proveedores-, podría dar lugar a que en la práctica fuese imposible determinar el origen del posible fallo o presentar ante los tribunales las pruebas necesarias para acreditarlo.

Con el propósito de incorporar al ordenamiento de la UE las soluciones a las cuestiones planteadas, el Parlamento Europeo emitió una Resolución de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA. El objetivo es cubrir la necesidad de adaptaciones específicas y coordinadas de los regímenes de responsabilidad civil para evitar situaciones en las que personas que sufran un daño o un menoscabo a su patrimonio debido a los sistemas de IA acaben sin indemnización.

Además, la Comisión Europea ha abierto la consulta pública para la reforma de la Directiva 85/374/CE del Consejo, en materia de responsabilidad por los daños causados por productos defectuosos, para adaptarla a la era digital, especialmente a la IA. El objetivo es que la reforma, prevista para el este año de 2022, complemente a la Ley de IA.

En el siguiente apartado se llevará a cabo un análisis de la resolución del Parlamento Europeo que busca establecer un régimen de responsabilidad civil en materia de IA para dar respuestas a la problemática jurídica de la implantación de máquinas y robots con estos sistemas integrados en el mercado laboral.

3.2. Propuesta Reglamento Responsabilidad Civil IA

El código civil español en su articulo 1902 regula que para el nacimiento de la responsabilidad civil exista una conducta negligente o culposa del causante del daño, es decir, el criterio de imputación de responsabilidad es fundado en la culpa del agente que causa el daño. En materia de responsabilidad civil por productos defectuosos, el principio general[46], el que será responsable es el productor o fabricante de este.

Ahora bien, se ha de precisar que la LGDCU[47] parte de la responsabilidad por culpa, en tanto en cuanto el fabricante sólo responde cuando es posible demostrar algún grado de culpa o negligencia en el proceso de fabricación y en el daño producido. En este contexto es difícil que el fabricante de un robot inteligente pueda garantizar una seguridad

[46] Artículos 135 y ss. del RD Legislativo 1/2007, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (LGDCU)

[47] Ley General para la Defensa de los Consumidores y Usuarios.

esperable, precisamente porque el punto de partida es que el robot es una máquina capaz de adoptar, como consecuencia del *machine learning* y de sus propias bases de datos, decisiones autónomas que no tienen interferencias humanas, que pueden resultar en acciones absolutamente imprevisibles.

Teniendo en cuenta esta situación el Parlamento Europeo venía trabajando en una nueva normativa que buscara establecer normas en relación con las demandas por responsabilidad civil de las personas físicas y jurídicas contra los operadores de sistemas de IA, en consecuencia, dictó una Resolución, de fecha 20 de octubre de 2020, que contiene recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA[48].

Esta propuesta se aplica a aquellos casos en que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA haya causado daños o perjuicios a la vida, la salud, la integridad física de una persona física y los bienes de una persona física o jurídica, o bien haya causado daños morales considerables que den lugar a una pérdida económica comprobable.

En materia de responsabilidad la ley distingue dos tipos de sistemas de IA, los de alto riesgo y los que no. Para los sistemas de alto riesgo, el artículo 4 establece que el operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA. Por otro lado, el operador de un sistema de IA que no constituya un sistema de IA de alto riesgo estará sujeto a responsabilidad subjetiva respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA, como regula artículo 8.

Esto significa que los operadores de sistema de IA de alto riesgo tienen que responder ante cualquier daño causado por sus sistemas a terceros con independencia de que tenga culpa el operador o fabricante. Es decir, al contrario de la normativa actual de producto defectuoso, que es necesario que el sujeto perjudicado acredite la existencia de defecto del producto, del daño sufrido y del nexo causal entre ambos, aquí con la simple existencia de un daño ocasionado por la IA el operador debe ser responsabilizado. La

[48] 2020/2014(INL)

responsabilidad civil del operador se basa en el hecho de que éste ejerce un grado de control sobre un riesgo asociado al funcionamiento y la operación de un sistema de IA.

En cambio, el operador de un sistema de IA que no sea de alto riesgo estará sujeto a un régimen de responsabilidad subjetiva[49]. En este caso, el operador no será responsable siempre y cuando pueda demostrar que no tuvo culpa o negligencia en el daño causado. Es decir, aunque se haya producido un daño a un tercero, se debe demonstrar la existencia de culpa o negligencia del operador.

Además, según se apartado 2) del articulo 8 de la propuesta existen dos motivos por los cuales el operador no será responsabilizado si puede demonstrar que no tuvo culpa en el daño ocasionado en caso de sistemas que no son de alto riesgo:

1. Activación del sistema de IA sin su conocimiento, aunque se llevara a cabo todas las medidas razonables y necesarias para evitarla.
2. Actuación diligente referente a la elección del sistema de IA a las tareas y capacidades pertinentes, correcta puesta en funcionamiento, el control de las actividades y el mantenimiento de la operativa mediante actualizaciones disponibles.

Cabe resaltar que tanto en el caso de los sistemas de alto riesgo como los que no, el operador no será responsable si la persona afectada o la persona de la que esta es responsable es la única a la que se le puede achacar el daño o perjuicio causado.

Con respecto a la concurrencia de varios operadores la propuesta plantea una responsabilidad compartida, estos serán responsables solidarios del pago de la indemnización en civil. Esto se traduce en que internamente, en la relación de los deudores, cada uno de ellos responde por la totalidad de la obligación, sin determinación de la parte correspondiente de cada.

También es cierto que en el articulo 12 de la propuesta, se regula que el operador que sea considerado responsable solidario con otros operadores en relación con una persona afectada y haya indemnizado íntegramente a esa persona afectada, de

[49] Artículo 8 de la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones

destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)).

conformidad con el artículo 4, apartado 1[50], o el artículo 8, apartado 1[51], podrá recuperar parte de la indemnización de otros operadores, en proporción a su responsabilidad. Los porcentajes de responsabilidad se basarán en los respectivos niveles de control por parte de los operadores sobre el riesgo relacionado con la operación y el funcionamiento del sistema de IA.

Existen, por tanto, dos regímenes de responsabilidad civil que convivirán al aprobarse la propuesta en materia de IA. Por un lado, las reglas generales de responsabilidad civil que engloban los Códigos Civiles, así como leyes específicas como la responsabilidad del fabricante. Por otro lado, se encuentra el régimen especial de responsabilidad civil previsto en la Propuesta de reglamento 2020. En este sentido, resulta lógico plantearse las interferencias que se pueden producir entre los regímenes.

El art. 2.3 de la Propuesta regula que éste régimen especial "se entiende sin perjuicio de cualquier otra demanda en materia de responsabilidad civil derivada de las relaciones contractuales, así como de la normativa sobre responsabilidad por los daños causados por productos defectuosos, la protección de los consumidores, la lucha contra la discriminación y la protección laboral y del medio ambiente, entre el operador y la persona física o jurídica que haya sufrido un daño o perjuicio a causa del sistema de IA y de que se pueda presentar contra el operador de conformidad con el Derecho de la Unión o nacional".

Esta declaración es matizada con relación a los sistemas de IA de alto riesgo, primero por el art. 4.5 de la propuesta, en caso de clasificación divergente sobre la responsabilidad objetiva, establece que el "Reglamento prevalecerá sobre los regímenes nacionales de responsabilidad civil en caso de clasificación divergente por responsabilidad objetiva de los sistemas de IA. Segundo con el art. 11, que para los dos tipos de responsabilidades regulados en la Propuesta se establece que "En caso de que haya más de un operador de un sistema de IA, estos serán responsables solidarios".

---

[50] Artículo 4 apartado 1) El operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA.

[51] Articulo 8 apartado 1) El operador de un sistema de IA que no constituya un sistema de IA de alto riesgo, tal y como se define en el artículo 3, letra c), y en el artículo 4, apartado 2, y que, en consecuencia, no figure en el anexo del presente Reglamento, estará sujeto a responsabilidad subjetiva respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA.

Además, también se especifica que "Si el operador inicial también tiene la condición de productor en el sentido del artículo 3 de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, deberá aplicársele dicha Directiva. Si solo hay un operador y dicho operador es también el productor del sistema de IA, el presente Reglamento prevalecerá sobre la Directiva sobre responsabilidad por los daños causados por productos defectuosos"[52]. "Si tanto el operador inicial como final tiene la condición de fabricantes, entonces, prevalecerá la legislación específica frente a la disciplina establecida por esta Propuesta. Finalmente, si solo hay un operador y es también fabricante del sistema, el régimen especial de la Propuesta de reglamento 2020 prevalece sobre la legislación en materia de responsabilidad del fabricante"[53].

El Parlamento entiende que la Directiva 85/374/CE del Consejo sobre responsabilidad por los daños por productos defectuosos puede aplicarse en relación con las reclamaciones por responsabilidad civil formuladas frente al productor de un sistema de IA defectuoso, en los supuestos comentados. El fabricante, programador, propietario o usuario del robot podrían beneficiarse de un sistema de responsabilidad limitada, siempre y cuando éste contribuya al fondo de compensación o bien suscriba conjuntamente un seguro que garantice la compensación de daños y perjuicios causados por los robots.

En definitiva, el esfuerzo normativo que se propone es importante para adecuar los avances tecnológicos a nuestra sociedad. La UE con esta propuesta establece el marco normativo necesario para determinar las responsabilidades de los agentes haciendo frente a uno de los grandes retos que plantea la IA.

V. CONCLUSIONES

Potenciar el desarrollo y la implantación de los sistemas de IA y proteger los derechos de las personas es lo que pretende la UE con las nuevas propuestas normativas. El trabajo es de gran envergadura y debe hacerse a la par de un desarrollo de normas técnicas por parte de las Organizaciones Europeas de Normalización, que tiene un reto

[52] Art. 11 de la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)).

[53] NAVAS NAVARRO, S. *Daños ocasionados por sistemas de inteligencia artificial*. Editorial Comares, Granada, 2022, pág. 112.

importante debido a la heterogeneidad de las tecnologías que incorporan los sistemas de IA.

Sin embargo, es indispensable no perder la oportunidad de proteger a los distintos operadores frente a los numerosos riesgos de violaciones de derechos que pueden producirse por el no acompañamiento del sistema jurídico a la nueva realidad surgida de la utilización de la IA. No cabe duda del potencial que tienen estos sistemas para mejorar la sociedad, optimizando el uso de recursos, siendo así más eficientes las empresas, con mayor precisión y mejorando la toma de decisiones por su potente capacidad analítica y en predicción de patrones, lo que aumenta la calidad etc.

La Ley de IA propone un marco jurídico basado en los tipos de riesgos de los sistemas inteligentes. Son estos que determinarán las obligaciones a cumplir por lo proveedores de los sistemas de IA para su desarrollo y comercialización en la UE. Además, la UE busca lograr con la Ley de IA que los sistemas de procesamiento de información y de datos que llevan a cabo los sistemas de IA cumplan con ciertos procesos de calidad para que los resultados sean los esperados, y que no se obtengan a costa de vulneraciones de derecho, sino que haya trasparencia e imparcialidad.

Por fin, en materia de responsabilidad civil, la propuesta del Parlamento Europeo establece una responsabilidad objetiva en caso de ser un sistema de IA de alto riesgo el que provoca el daño, que se traduce en que el fabricante tiene que responder ante cualquier daño causado por sus sistemas a terceros con independencia de que tenga culpa el operador o fabricante. Por el contrario, si se trata de un sistema que no genere un alto riesgo, el operador estará sujeto a un régimen de responsabilidad subjetiva, es decir, el operador no será responsable siempre y cuando pueda demostrar que no tuvo culpa o negligencia en el daño causado.

VI. BIBLIOGRAFÍA

AISLINN, K. “The AI Act and algorithmic management”, op. cit. p. 3, disponible en https://cllpj.law.illinois.edu/content/dispatches/2021/Dispatch-No.-39.pdf

BAJO, J.C. “El uso profesional de los drones y la prevención de riesgos laborales” en Revista web MC Salud Laboral, abril 2021, págs. 18 a 23, disponible en https://prevencion.mc-mutual.com/articulos/-

/asset_publisher/gPV7bp1C7xJS/content/el-uso-profesional-de-los-drones-y-la-prevencion-de-riesgos-laborales.

BERENGUER BIRD & BIRD, P. "Inteligencia artificial: ¿quién debería responder de los daños que cause una máquina?" en *Periódico La Expansión*. 15 diciembre de 2021. Disponible en https://www.expansion.com/juridico/opinion/2021/12/15/61ba2161e5fdea28638b45b0.html

BUCHANAN, B. AND MILLER, T., *Machine Learning for Policymakers*: *What It Is and Why It Matters,* Harvard Kennedy School, Belfer Center for Science and International Affairs, June 2017, disponible en https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf

CALO, R. "Robotics and the Lessons of the Cyberlaw", 103, Cal. L. Rev. 2015, p.513 y ss, *UW Law Digital Commons*, disponible en https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1022&context=faculty-articles

CAZALILLA RUIZ, M. "La responsabilidad civil derivada del uso de la inteligencia artificial" en Noticias Jurídicas, 29 de julio de 2021.

EU-OSHA, "Artificial intelligence for worker management: implications for occupational safety and health - Executive Summary", 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" julio de 2020, disponible en https://osha.europa.eu/es/publications/smart-personal-protective-equipment-intelligent-protection-future

EUROPEAN COMMISSION (December 2016), *Study on Big Data in Public Health*, Telemedicine and Healthcare, disponible en https://wayback.archive-it.org/12090/20170117023306/https://ec.europa.eu/health/sites/health/files/ehealth/docs/bigdata_report_en.pdf.

EUROPEAN COMMISSION, "Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", COM (2021) 206 final.

FEMEVAL, *Guía de Drones en Prevención de Riesgos Laborales*, disponible en https://www.femeval.es/dam/jcr:b1859d99-e78f-44e0-aaac-d4e65d50697c/GUIA%20DRONES.pdf

FEMEVAL, *Guía de Fabricación Aditiva en Prevención de Riesgos Laborales*, disponible en https://www.femeval.es/dam/jcr:aa78cfcc-5068-4abd-8999-9c6c1d201e4d/GUIA-FABRICACION-ADITIVA.pdf

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

FEMEVAL, *Guía de Robot Industriales y Cobots en Prevención de Riesgos Laborales*, disponible en https://www.femeval.es/dam/jcr:fd091e5f-3c97-42fd-9981-680e8232a645/GUIA_ROBOTS.pdf

FEMEVAL, *Guía de Sistemas IoT en Prevención de Riesgos Laborales*, disponible en https://www.femeval.es/dam/jcr:be830229-384d-45fd-909e-4a60d2ef5b71/GUIA%20IOT.pdf

GOÑI SEIN, J.L. "Ley de inteligencia artificial y seguridad y salud en el trabajo" 2022*, en prensa*.

HERNÁNDEZ RAMOS, C. "Responsabilidad por productos defectuosos en la Unión Europea. Comentarios sobre un antes y un después de la expedición de la directiva 347 de 1985" en *Revist@ E-Mercatoria*, Vol.17, N.º 1, enero-Junio/2018, Págs. 87-121.

JOYANES. AGUILAR, L. *Industria 4.0: La cuarta revolución industrial*. Alfaomega Grupo Editor, S.A de C.V., México, 2017, págs. 2 y 27.

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

NAVAS NAVARRO, S. *Daños ocasionados por sistemas de inteligencia artificial*. Editorial Comares, Granada, 2022, pág. 112.

NAVAS NAVARRO, S. "Smart robots y otras máquinas inteligentes en nuestra vida cotidiana" en *Revista CESCO de Derecho de Consumo*, N.º 20/2016, disponible en https://revista.uclm.es/index.php/cesco/article/view/1249/1028

OLIVA LEÓN, R. "Inteligencia artificial y responsabilidad civil por daños" en Algoritmo Legal, 2020 (actualizado 28 de enero de 2022), disponible en https://www.algoritmolegal.com/tecnologias-disruptivas/responsabilidad-civil-y-danos-causados-por-la-inteligencia-artificial-propuesta-del-parlamento-europeo/

ON AIR, "Nuevo reglamento europeo de drones 2021" disponible en https://www.oneair.es/nuevo-reglamento-europeo-drones/#947, consultado en septiembre 2022.

PONCE, A. "The AI Regulation: Entering an AI Regulatory Winter? Why An Ad Hoc Directive on Ai in Employment Is Required", *ETUI Research Paper* - Policy Brief 2021.07.7, disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873786

VÁZQUEZ BULLA. C. "La responsabilidad civil por productos defectuosos a la luz de la nueva Ley 3/2014: pasado, presente y futuro desde la perspectiva legal, doctrinal y jurisprudencial" en *Revista de Derecho UNED*, núm. 14, 2014. Págs. 717 y ss.

VICENT SELVA, B. "Cuarta Revolución Industrial" consultado en agosto de 2022, disponible en https://economipedia.com/definiciones/cuarta-revolucion-industrial.html

ZORRAQUINO, A. "Resumimos la propuesta europea de Reglamento sobre los usos de la Inteligencia Artificial" en *Periscopio Fiscal y Legal*, 4 de mayo de 2021, disponible en https://periscopiofiscalylegal.pwc.es/europa-presenta-su-propuesta-de-reglamento-sobre-los-usos-de-la-inteligencia-artificial/

WTW, *Realidad virtual, aumentada y mixta: la cadena del riesgo se vuelve más compleja*, disponible en https://willistowerswatsonupdate.es/ciberseguridad/realidad-virtual-aumentada-mixta-riesgos/