

¿Estamos caminando hacia el reconocimiento de la personalidad jurídica a los robots en la Unión Europea?

Are we moving towards the recognition of legal personality for robots in the European Union?

Susana CHECA PRIETO

EAE Business School (España)
scheca@eae.es

Recepción: Octubre 2021
Aceptación: Febrero 2022

RESUMEN

La IA es una tecnología estratégica que puede reforzar la competitividad de la industria europea y mejorar el bienestar de los ciudadanos. Para que su desarrollo sea un éxito en la UE es imprescindible desarrollar un marco jurídico seguro y adecuado, sin frenar el desarrollo tecnológico.

Una de las primeras cuestiones que se planteó fue la posibilidad del reconocimiento de personalidad jurídica a los robots. A pesar del acalorado debate inicial, actualmente únicamente contamos con una Propuesta de Reglamento de la Comisión Europea sobre el marco jurídico aplicable a los sistemas de IA, que incluye una regulación de los sistemas de alto riesgo y reglas de transparencia armonizadas sobre los sistemas dirigidos a interactuar con personas físicas.

El objetivo de este artículo es analizar si las modificaciones legislativas están afrontando dichos retos o si, por el contrario, el sistema propuesto queda lejos de solucionar las cuestiones planteadas.

Palabras clave: inteligencia artificial, política pública, derechos, riesgos, Unión Europea.

Clasificación JEL: K23

ABSTRACT

AI is a strategic technology that can strengthen the competitiveness of European industry and improve the well-being of citizens. For its development to be a success in the EU, it is essential to develop a safe and adequate legal framework, without slowing down technological development.

One of the first issues raised was the possibility of legal personality recognition for robots. Despite the heated initial debate, we currently only have a Proposal for a Regulation from the European Commission on the legal framework applicable to AI systems, which includes a regulation of high-risk systems and harmonized transparency rules on systems aimed at interaction with natural persons.

The objective of this article is to analyse if the legislative modifications are facing these challenges or if, on the contrary, the proposed system is far from solving the issues raised.

Keywords: artificial intelligence, public policy, rights, risks, European Union.

JEL Classification: K23



1. INTRODUCCIÓN

1.1 Planteamiento del problema

Desde la utilización de la palabra *robot* por Karel Capek en la obra *Robots Universales Rossum* de 1920 (Somolinos Sánchez, 2002: 32), hemos asistido a un avance imparable que ha desembocado en el nacimiento de la IA.

A día de hoy existen múltiples aplicaciones con IA como, por ejemplo, asistentes personales, traducciones instantáneas en dispositivos, fotografías con Inteligencia Artificial (IA), servicios con recomendaciones, chatbots, software para detectar el cáncer o alimentos con IA. En este sentido, Smith (2019: 17) realiza una investigación sobre las diferentes acepciones y limitaciones de lo que actualmente se entiende por IA.

Unos años antes, en 2013, Marc Tarabella, miembro del Parlamento Europeo, introdujo la problemática sobre el derecho de los robots, bajo los siguientes interrogantes: (i) ¿Cuál es la realidad de la situación? (ii) ¿Cuál es el objetivo? (iii) ¿Cuál es el presupuesto en esa área? A raíz de estas preguntas surgió el proyecto *Robolaw*¹, con el objetivo de proporcionar un marco de referencia a los operadores del sector, y así inspirar una regulación avanzada que pueda impulsar el surgimiento de la robótica y asegurarle un desarrollo congruente con los valores propios del orden jurídico europeo (Palmerini, 2017).

19

Actualmente no es posible negar los beneficios potenciales de la IA que, de hecho, son ya de aplicación en prácticamente cualquier ámbito de nuestra vida; desde la atención a personas, a la educación, pasando por los momentos de ocio.

Sin embargo, desde que en febrero de 2017 el Parlamento Europeo aprobara unas recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica², no se había vuelto a saber mucho más sobre este tema, ni siquiera sobre la evolución de su tramitación.

Una de las primeras cuestiones que se planteó en el debate sobre la necesidad de que la Unión Europea desarrollara una legislación específica sobre IA fue la posibilidad del reconocimiento de personalidad jurídica a los robots.

¿Deberían ser los robots considerados verdaderas personas? En caso de responder afirmativamente a esta pregunta, cobraría sentido la propuesta de que los “*trabajadores robots*” de Europa puedan ser clasificados como “*personas electrónicas*” y, en consecuencia, de que sus propietarios sean responsables de pagar la seguridad social por ellos, así como asumir una responsabilidad legal por sus acciones.

De hecho, cuestiones importantes en el ámbito laboral a día de hoy como, por ejemplo, el control horario o el absentismo laboral quedarían, obviamente, resueltas de inmediato con las jornadas de trabajo de los robots persona.

El reconocimiento de personalidad jurídica a los sistemas de IA tendría consecuencias sobre todas las ramas del Derecho, por lo que esta tesis conllevaría la necesidad de dotarnos de nuevas normas, en lugar de aplicar soluciones ya conocidas, en especial en lo que a responsabilidad por daños se refiere.

Sin embargo, la doctrina no es uniforme sobre la consideración jurídica que debe otorgarse a los sistemas de IA y, en concreto, a los robots.

Así, Calo (2015: 515) considera que los robots pertenecen a una categoría ontológica nueva, siempre que partamos de una sistematización que predica de la robótica tres propiedades privativas (2016: 187):

- Corporeidad: el robot tiene una materialidad corpórea, lo que no se puede afirmar del software.
- Impredecibilidad: el robot piensa y decide con cierta autonomía, a diferencia de una simple máquina.
- Impacto social: las personas se preocupan por la situación de determinados androides o, incluso, por sus derechos.

Si bien es cierto que las personas no tienden a considerar a los robots humanoides como seres vivos, tampoco entienden que sean objetos. Por ello, Calo (2015: 518) alude una nueva categoría de sujeto jurídico a medio camino entre persona y objeto, siendo su calificación parcial y su asignación incompleta, contextual e inestable, en tanto en cuanto los ciudadanos puedan tratar al robot como persona para algunos propósitos y como objeto para otros.

Por su parte, Barrio Andrés (2019: 34) se muestra favorable a un Derecho de los Robots con objeto de distribuir los derechos y responsabilidades que surgen de las acciones de los seres no humanos y regular el impacto social que conlleva la sustitución de seres humanos por sistemas de IA. Desde su punto de vista, la característica que une a los nuevos “artefactos” es su capacidad de actuar físicamente sobre el mundo real y, en consecuencia, de dañar materialmente a las personas y a las cosas.

Barrio Andrés (2019: 37) considera que la regulación existente no da respuesta a los desafíos que surgen ante esta nueva realidad, ni desde el punto de vista jurídico, ni social, económico, de salud o ético. Por ello, considera evidente la urgente necesidad de definir las condiciones de legitimidad jurídica de las nuevas invenciones y establecer con precisión un régimen claro de derechos y obligaciones.



Frente a estas posturas, quizás la posición más acertada sea la de Lacruz Mantecón (2019: 25) quien afirma que “quizás sea más adecuado no precipitarse y considerar que la originalidad de este Ciberderecho va a ser la misma que la que pueda encontrarse en disciplinas como el Derecho de la circulación, es decir, que estamos ante un medio que conjugará cierta especialización pero que no va a crear nada que no exista con anterioridad”. Recuerda este autor algún manual de principios del siglo XX donde se lee como posible disciplina del Derecho privado la del Derecho de la telefonía y considera que sucede algo similar a día de hoy con el Derecho de Internet.

El debate sobre el reconocimiento de una “*personalidad electrónica*” sigue abierto a día de hoy y, en este contexto, la UE ya ha diseñado un marco jurídico con el objetivo de que dotar de confianza a los ciudadanos y seguridad jurídica a las empresas, de forma que no se ralentice la adopción de las tecnologías de IA, si bien en dicho marco jurídico no se contempla esta opción.

Nos estamos refiriendo, en concreto, al Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza-³ objeto de consulta pública abierta hasta el 19 de mayo de 2020, y a la reciente a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021⁴.

21

Ya en el proyecto de informe al Parlamento Europeo con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica⁵, presentado el 31 de mayo de 2016 por la diputada Mady Delvaux de la Comisión de Asuntos Jurídicos, se introdujo la idea de un impuesto a los robots, generando un rechazo prácticamente unánime.

En el proyecto de informe de 31 de mayo de 2016 en ningún momento se indica la conveniencia de que los robots con “*persona electrónica*” deban cotizar a la Seguridad Social, sino que literalmente la propuesta versaba sobre la necesidad de que “*habida cuenta de los efectos que el desarrollo y la implantación de la robótica y la inteligencia artificial podrían tener en el empleo y, por ende, en la viabilidad de los sistemas de seguridad social de los Estados miembros, debería examinarse la necesidad de exigir a las empresas que informen acerca de en qué medida y proporción la robótica y la inteligencia artificial contribuyen a sus resultados económicos, a efectos de fiscalidad y del cálculo de las cotizaciones a la seguridad social*”.

Una sugerencia similar la encontramos en el Informe de 27 de enero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre robótica⁶.

Finalmente, la Resolución del Parlamento Europeo de 16 de febrero de 2017 únicamente incluye lo siguiente: *“Destaca la importancia que reviste la previsión de los cambios sociales, habida cuenta de los efectos que podrían tener el desarrollo y la implantación de la robótica y la inteligencia artificial, pide a la Comisión que analice los diferentes posibles escenarios y sus consecuencias para la viabilidad de los sistemas de seguridad en los Estados miembros”*.

Por lo tanto, estrictamente desde el punto de vista del marco normativo europeo, no existe debate ni intención, a día de hoy, no solo de reconocer dicha *“personalidad electrónica”* a los robots, sino ni siquiera de desarrollar un marco impositivo en el que se tenga en cuenta en la facturación de las empresas, a efectos tributarios y de cotización a la seguridad social, la introducción de los robots.

Dedicaremos, pues, las siguientes páginas, a analizar qué ámbitos del Derecho resalta la doctrina como aquellos más afectados por el desarrollo de los sistemas de IA y cuál es la respuesta que proporciona actualmente el Derecho de la UE para, finalmente, determinar si el marco jurídico desarrollado efectivamente da respuesta a los desafíos planteados por esta nueva realidad.

22

1.2 Definición de robot de la Unión Europea

Hintze (2016) diferencia entre cuatro tipos en los que se pueden clasificar los sistemas dotados de IA:

- a) Máquinas reactivas: no tienen memoria y no pueden utilizar experiencias pasadas para la toma de decisiones, de forma que actúan en función de lo que ocurre en cada momento. Por lo tanto, ante situaciones idénticas, actúan de igual forma.

Este tipo de máquinas son adecuadas para, por ejemplo, jugar a algunos juegos, pero no pueden ser utilizadas para otras distintas. Un ejemplo sería Deep Blue, la máquina que compite en ajedrez, que toma sus decisiones en función de la disposición de las fichas en el tablero en cada momento, pero no recuerda partidas anteriores.

- b) Máquinas con memoria limitada. No son capaces de aprender, pero sí de almacenar datos pasados como, por ejemplo, los coches autónomos, capaces de conducir solos.
- c) Máquinas con una teoría de la mente: son capaces de entender y expresar ideas, pueden trabajar en equipo y adaptar su comportamiento a lo que ocurre a su alrededor. Estas máquinas son las que en un futuro serán capaces de entender las diferencias entre las personas para tratarlas de uno u otro modo.
- d) Máquinas con conciencia propia que, a partir de sus estados internos, pueden predecir comportamientos y sentimientos ajenos. Si una máquina ha



experimentado amor hacia una persona, podrá entender que otra persona esté enamorada. Así mismo, pueden construir una representación de sí mismas.

Antes de avanzar en el análisis de las bases del régimen normativo aprobado tras la publicación del Libro Blanco sobre inteligencia artificial, y la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de IA (Ley de Inteligencia Artificial), debemos recordar la definición de la Comisión sobre los sistemas de IA:

“programas informáticos (y posiblemente también equipos informáticos) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado”⁷.

Partiendo de esta definición, encontramos los siguientes elementos necesarios identificados por la Unión Europea para que un sistema pueda considerarse robot o sistema de IA por parte de la Unión Europea:

- Programas y/o equipos informáticos,
- Capaces de percibir su entorno de las siguientes formas:
 - Adquisición de datos estructurados o no,
 - Interpretación de dichos datos
- Razonamiento sobre el tratamiento de los datos, y
- Decisión de acciones para alcanzar el objetivo fijado.

Uno de los mayores problemas a los que nos enfrentamos a la hora de definir qué es un sistema de IA es que debe ser lo suficientemente flexible para adaptarse al progreso técnico, a la vez que mantiene un nivel de precisión adecuado para ofrecer la seguridad jurídica necesaria.

De hecho, si comparamos esta definición con la que establece la RAE, ésta limita la IA a la disciplina que crea programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico. Es decir, los equipos informáticos quedan al margen de la definición que la RAE nos proporciona.

Por otra parte, tampoco incluye la definición de la UE ninguna referencia a la comparación con las operaciones que realiza la mente humana. Esta eliminación resulta, desde nuestro punto de vista, acertada, en tanto en cuanto las operaciones que llevan a cabo los sistemas de IA no imitan comportamientos humanos basados en emociones o sentimientos.

En lo que hay acuerdo a día de hoy es en que no se han desarrollado sistemas de IA que tengan conciencia de sí mismos, en el sentido de reconocerse como entes independientes y capaces de tomar decisiones, diferenciando entre sí mismos y los objetos, personas o sistemas que les rodean.

2. ÁMBITOS DEL DERECHO AFECTADOS

Como anteriormente hemos indicado, la utilización de los sistemas de IA afecta ya, en mayor o menor grado, a la vida diaria de los ciudadanos, con independencia de que seamos o no plenamente conscientes de ello y, especialmente, de las consecuencias jurídicas que ello pueda generar.

En este sentido, consideramos esencial realizar un breve análisis de los ámbitos del Derecho afectados, con el fin de determinar la adecuación del marco jurídico elaborado por la Unión Europea y plantear, si bien no siempre resolver, los interrogantes que la introducción de los sistemas de IA plantea actualmente.

2.1. Derecho internacional

24

Como pone de manifiesto García San José (2021: 260), uno de los grandes problemas que se deben abordar desde el Derecho Internacional es la actual indeterminación de lo que debe entenderse por IA, que se evidencia a nivel institucional, junto con la opacidad que rodea el sector y la consiguiente imprevisibilidad de sus riesgos. De acuerdo con este autor todo ello dificulta, si bien no imposibilita, una eventual regulación internacional de la IA.

Las vías con las que el derecho internacional cuenta van desde el *hard law* (por medio de tratados), la armonización del *soft law* (mediante códigos de conducta), o la vía intermedia que supondría la interpretación jurisprudencial teleológica de los tratados en vigor.

Sin embargo, García San José se decanta por la vía de estandarización del *Global Law* (principios informadores) como respuesta sobre una base consensual colectiva, aplicando el principio de necesidad como principio general del Derecho Global, vinculado al principio informador de la dignidad intrínseca del ser humano como piedra angular de un cuerpo jurídico internacional del que se derivasen obligaciones jurídicas vinculantes para todos los actores que participan en el ciclo de vida de los sistemas de IA.

Dada la indiscutida validez universal del principio informador de la dignidad intrínseca del ser humano, solo habría que releerlo en el contexto de los desafíos y riesgos que suscita la IA a la luz de otro emergente principio general del Derecho internacional, como es el principio de necesidad.

Debemos señalar, a este respecto, la reciente adopción del primer marco ético sobre inteligencia artificial, Recomendación sobre la Ética de la Inteligencia Artificial,



aprobado en la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), reunida en París del 9 al 24 de noviembre de 2021, en su 41ª reunión, por sus 193 Estados miembros⁸.

La Recomendación tiene objetivo hacer realidad las ventajas que aporta la IA, reduciendo los riesgos que conlleva de forma que se garantice que las transformaciones digitales promueven los derechos humanos y contribuyen a la consecución de los Objetivos de Desarrollo Sostenible, abordando cuestiones relativas a transparencia, rendición de cuentas y privacidad.

En cuanto a protección de datos, la Recomendación es exigente en cuanto pide que se actúe más allá de lo que hacen las empresas tecnológicas y gobiernos, con el objetivo de garantizar a las personas una mayor protección, asegurando la transparencia, la capacidad de actuar y el control de sus datos personales.

En este sentido, la Recomendación afirma que todos los individuos deberían poder acceder a sus registros de datos personales e incluso borrarlos, partiendo del conocimiento y del derecho del individuo a controlar sus propios datos.

25

Con el fin de conseguir esta finalidad, la Recomendación aumenta la capacidad de los organismos reguladores de todo el mundo para hacerla cumplir.

Desde el punto de vista de los sistemas de IA para vigilancia masiva y calificación social, quedan explícitamente prohibidos por la Recomendación, dado la vulneración para los derechos humanos y libertades fundamentales que supone su uso generalizado.

Desde el punto de vista de la aplicación práctica de la Recomendación, se incluye una Evaluación de Impacto Ético para ayudar a los países y a las empresas que desarrollan sistemas de IA a evaluar el impacto de estos sistemas en las personas, la sociedad y el medio ambiente. Esta metodología también ayudará a los Estados miembros a evaluar su grado de preparación en términos de infraestructura jurídica y técnica, ayudando a mejorar la capacidad institucional de los países y a recomendar medidas adecuadas que deben adoptarse.

En este sentido, la Recomendación anima a los Estados miembros a considerar la posibilidad de contar con un funcionario independiente de ética de IA u otro mecanismo para supervisar los esfuerzos de auditoría y seguimiento continuo.

Otra de las cuestiones fundamentales abordadas por la Recomendación es la lucha contra el cambio climático y el tratamiento de los problemas medioambientales. La Recomendación, además de pedir a los gobiernos que evalúen el impacto medioambiental directo e indirecto a lo largo del ciclo de vida los sistemas de IA, instruye a los gobiernos

a no utilizar un sistema de IA que tenga un impacto negativo desproporcionado de los sistemas de IA en el medio ambiente.

Por lo tanto, las modificaciones de las legislaciones nacionales deben ajustarse a las obligaciones de los Estados miembros en materia de derechos humanos y promover las libertades fundamentales a lo largo del ciclo de vida de estos sistemas, promoviendo iniciativas de gobernanza, buenos ejemplos de prácticas de colaboración en relación con los sistemas de IA y directrices técnicas y metodológicas nacionales e internacionales a medida que avancen estas tecnologías.

Es muy interesante constatar, a efectos de nuestro artículo, como la Recomendación subraya que, a la hora de desarrollar marcos normativos, los Estados miembros deben tener en cuenta que la responsabilidad última y rendición de cuentas debe recaer siempre en los seres humanos, no debiendo otorgarse personalidad jurídica a las tecnologías de IA por sí mismas.

Para lograr esta Recomendación, los marcos reguladores deberían ajustarse al principio de supervisión humana y establecer un enfoque global centrado en los actores de la IA y los procesos tecnológicos que intervienen en las diferentes etapas del ciclo de vida de los sistemas de IA.

2.2.Derecho constitucional

Resaltan Serrano Pérez y Fernández Aller (2021: 160) que, dentro de todos los posibles temas pendientes de reflexión en el Derecho constitucional, destaca el de los conflictos entre la IA y los derechos fundamentales y, en especial, el derecho a la protección de los datos personales (art. 18.4 CE) y a la privacidad, el derecho a la intimidad (art. 18.1 CE), el derecho a la igualdad (art. 14 CE) y a la no discriminación por razón de sexo, raza, religión, opinión, discapacidad, edad, orientación sexual, etc.

En cualquier caso, desde la óptica de estas autoras, además de los derechos anteriormente señalados, el mal uso de la IA puede dañar cualquier derecho (desde la libertad de circulación al derecho al trabajo, o a la educación).

En este sentido, a pesar de los beneficios sustanciales que la IA aporta a las personas y a la sociedad, no podemos olvidar los efectos negativos que puede tener sobre valores como la democracia, el Estado de Derecho o la justicia distributiva.

En consecuencia, a pesar de la importancia de la autorregulación y el desarrollo de códigos éticos por parte de las empresas, especialmente las tecnológicas, estas autoras consideran imprescindible contar con principios jurídicos fuertes de aplicación en el ámbito constitucional.



En el propio Libro Blanco sobre la inteligencia artificial se pone de manifiesto riesgos potenciales de la IA como la opacidad en la toma de decisiones, la discriminación de cualquier tipo, la intromisión en la vida privada o su uso con fines delictivos y, en este sentido, se hace imprescindible una nueva perspectiva constitucional para otorgar consistencia jurídica a esta nueva realidad, en un entorno europeo común que habrá de tener en cuenta los principios que derivan del Estado social y de Derecho.

Por lo tanto, en opinión de estas autoras, la transparencia es una de las características a las que más atención debe prestar el Derecho, pero, además, han de surgir nuevos derechos a los que ha de dar forma y protección el Derecho constitucional como, por ejemplo, el derecho a la no discriminación algorítmica, derecho a la explicabilidad y los neuroderechos.

El Derecho constitucional, esto es, el respeto a los derechos fundamentales y a los valores constitucionales, también consagrados por la UE es, desde el punto de vista de estas autoras, el sustrato común sobre el que construir la IA.

Una de las grandes paradojas de la IA es que no puede ofrecer una explicación detallada de cómo se llega a un determinado resultado, es decir, no siempre puede establecerse cómo el algoritmo evalúa y pondera los datos y la información que procesa, dando lugar al fenómeno denominado “caja negra”. Como indica Barrat (2014: 32) se llama sistema de “caja negra” a la herramienta computacional en la que uno entiende los datos ingresados y los resultados, pero no entiende el procedimiento subyacente. Aquí el código es inescrutable porque el programa evoluciona y los humanos no pueden entender el proceso que siguió la programación para lograr una solución determinada.

No podemos olvidar, como muy acertadamente señala Corvalán (2017: 41), que el modelo de derechos humanos se cristaliza a partir de un paradigma que se basa en asignar el carácter de inalienable e inderogable a los derechos esenciales de la persona, existiendo una vinculación directa entre estos derechos y la dignidad humana, la paz, la protección de las minorías, de los más vulnerables o de los más débiles.

Partiendo de esta base, para que el desarrollo de la IA sea compatible con el modelo de derechos humanos, Corvalán señala como imprescindible una regulación que incorpore una serie de principios para hacer más robusto el sistema de protección, a saber:

- a) Autodeterminación algorítmica: este principio se deriva de la dignidad la persona humana y trata de asegurar el libre desarrollo de la personalidad a partir de reconocer la autodeterminación informativa para garantizar el derecho a elegir, el derecho a saber, al conocimiento y a la autorregulación de la información.

Como la IA intermedia cada vez más entre los datos y las decisiones de las personas, resulta imprescindible proteger sus derechos promoviendo el respeto de los principios de

necesidad, finalidad, proporcionalidad y pertenencia de datos personales (Rodotá, 2014: 154).

- b) Máxima transparencia algorítmica: este principio se vincula a la prohibición de las “cajas negras” anteriormente descritas. La IA debe ser transparente en sus decisiones, pudiéndose deducir una explicación entendible de los criterios utilizados para alcanzar un determinado resultado.
- c) No discriminación algorítmica: este principio implica que el diseño y la implementación de los algoritmos inteligentes deben respetar el principio de no discriminación, es decir, se debe impedir que las máquinas basadas en sistemas de IA procesen los datos aplicando sesgos por motivos de raza, sexo, idioma, religión, opinión política, origen, condición social, etc.

En conclusión, sostiene Corvalán, parece clara la necesidad de impulsar un marco regulatorio vinculado a los sistemas de IA, de forma similar al que se dio con el surgimiento de las Tecnologías de la Información y las Comunicaciones en el ámbito de la ONU, de forma que el desarrollo de la IA sea compatible con los derechos humanos, garantizando la intervención humana frente a las predicciones y decisiones de los algoritmos, de forma que el procesamiento de la información sea legítimo y respetuoso con la efectividad de los derechos de las personas.

2.3.Derecho civil

Quizás sea el Derecho civil una de las áreas centrales de análisis, en tanto en cuanto sus normas establecen las condiciones que se deben cumplir para el reconocimiento de personalidad a las personas físicas y jurídicas.

El planteamiento que realiza González Granado (2016) es si, teniendo en cuenta la normativa vigente, existe actualmente la posibilidad de adscribir los robots autónomos inteligentes a una categoría jurídica existente o, en su caso, es necesario crear una categoría específica acorde con sus especialidades.

En este sentido, Santos González (2017: 40), examina su posible encaje en alguna de las ya existentes.

En primer lugar, su consideración como persona física exige el cumplimiento de los requisitos del artículo 30 del Código Civil conforme al cual la personalidad se adquiere desde el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno. Obviamente, el elemento biológico en ningún caso puede predicarse de los sistemas de IA o robots, por lo que no es posible encuadrarlos en esta categoría.



Por su parte, el artículo 35 del Código Civil define como persona jurídica a las corporaciones, asociaciones y fundaciones de interés público reconocidas por la ley, así como las asociaciones de interés particular, sean civiles, mercantiles o industriales, a las que la ley conceda personalidad propia, independientemente de la de cada uno de los asociados.

Por otra parte, la equiparación de los robots a los animales se ve imposibilitada por la carencia de base biológica, así como por el hecho de que, a día de hoy, los robots no pueden experimentar sentimientos.

Desde el punto de vista de este autor, además del hecho de que los sistemas de IA carezcan de cuerpo físico, el hecho de que puedan actuar directamente con su entorno, a diferencia de las personas jurídicas que lo hacen a través de sus representantes, impide su equiparación desde un punto de vista sustantivo. Podrían, en todo caso, llegar a existir similitudes en el sentido de encontrarnos ante una ficción jurídica de la personalidad.

No existe duda de que cabría considerar “cosa” o “bien” a los robots de primera, segunda y tercera generación. Sin embargo, como reconoce por la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica “cuanto más autónomos sean los robots, menos se les podrá considerar simples instrumentos en manos de otros agentes”.

29

Ante esta situación, García Sánchez (2020: 61) concluye que sí será necesaria la creación de una categoría intermedia entre las cosas y las personas físicas, que aúne las especialidades de estos sistemas de IA, para lo que es imprescindible determinar específicamente las particularidades concretas que deben tenerse en cuenta.

Sin embargo, dentro del seno de la UE, el Comité Económico y Social Europeo, en su Dictamen Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad⁹, se opone a cualquier tipo de estatuto jurídico para los robots o sistemas de IA “por el riesgo moral inaceptable que ello conlleva”. Considera, así, que la legislación en materia de responsabilidad tiene un efecto correctivo y preventivo que podría desaparecer si el riesgo de responsabilidad civil dejase de recaer sobre el autor para ser transferido al robot o sistema de IA.

Nos estamos centrando, específicamente, en los denominados robots de cuarta generación caracterizados por lo que se entiende por una “Inteligencia Artificial Fuerte”, es decir, aquellos sistemas capaces de emular el funcionamiento de la mente humana, incluyendo no solo la capacidad de resolución de tareas, sino también los sentimientos, la creatividad y la auto-conciencia.

Según sus defensores, la relación entre el espíritu y el cerebro es del mismo orden que aquella que existe entre el software y el hardware, tal como defiende Daniel C. Dennett (1995:41).

Sin embargo, tras la propuesta del Parlamento Europeo en su Resolución de 2017 en la que se alude como una de las posibles soluciones (Recomendación 59.f) para hacer frente a los supuestos de responsabilidad por daños ocasionados por robots a la creación a largo plazo de una personalidad jurídica específica, 285 expertos de 14 países dirigieron una carta abierta al Presidente de la Comisión Europea y resto de dirigentes europeos, en la que manifestaban su rechazo al reconocimiento de esta personalidad (<http://www.robotics-openletter.eu/>).

En concreto, si el estatus legal de un robot derivara del modelo de persona natural, debería ostentar derechos humanos tales como la dignidad, integridad, remuneración o ciudadanía, lo que se enfrenta a la tradicional concepción de los derechos humanos, a la Carta de los Derechos Fundamentales de la Unión Europea y a la Convención para la protección de los Derechos Humanos y las Libertades Fundamentales.

30

En este mismo sentido se manifiesta González Granado (2016), quien indica que las referencias a los valores humanistas son una constante citada en todos aquellos textos contrarios a la consideración de los sistemas de IA como sujetos de derechos.

Coincide con él Nevejans (2016: 16), quien afirma que el reconocimiento de una personalidad electrónica a los robots pondría en tela de juicio los fundamentos humanistas de Europa.

Brokek y Jakubiec (2017: 303), por su parte, defienden que, si bien sería posible admitir un nuevo estatus legal para las máquinas autónomas desde un punto de vista meramente técnico, en la práctica permanecería como un mero derecho de libro sin materialización real.

Sin embargo, Quintero Olivares (2017: 9) sí defiende la posibilidad de que existan normas que partan de la ficticia personalidad del robot y permitan reconocerle responsabilidad, de la misma forma que históricamente el Derecho ha relativizado el vínculo ser humano-persona, negando tal condición a los esclavos, o atribuyendo a masas de bienes u organizaciones administrativas.

Por lo tanto, en caso de incluirse a los robots en un cuarto nivel de las categorías jurídicas existentes, habría que delimitar el contenido de dicha personalidad electrónica.



A este respecto, García Mexía (2016) descarta tajantemente que se puedan conceder a las personas electrónicas los derechos constitucionales, predicables únicamente de los seres humanos.

No sería tan complejo reconocerles determinados derechos patrimoniales, como los derechos de autor, tal como ha hecho la sentencia de un tribunal de Shenzhen –provincia china de Guangdong–, que determinó que un artículo escrito por un algoritmo de IA desarrollado por la compañía Tencent debía recibir la misma protección a nivel de derechos de autor que los textos creados por seres humanos¹⁰.

En efecto, tal como afirma García Sánchez (2020: 60) dado que nuestra vigente Ley de Propiedad Intelectual¹¹ ya reconoce derechos de propiedad intelectual a las personas jurídicas en determinadas situaciones, el avance de esta tecnología podrá traer un desarrollo normativo posterior atribuyéndole la condición de autor a los inventores por la obra de los sistemas de su creación, siéndoles también exigibles una serie de obligaciones.

2.4.Derecho administrativo

Cerrillo i Martínez (2019: 61) repasa distintos ejemplos de sistemas de IA utilizados por las administraciones públicas en tareas tales como predecir el riesgo de incendio de los edificios (Atlanta) o de riadas (Hampton) o identificar los locales que serán objeto de inspección (Las Vegas, Chicago). También se utiliza en la personalización de servicios a partir del análisis de los datos personales de los ciudadanos y del comportamiento de otros usuarios a partir de la creación de perfiles (MyGov Social del Consorci Administració Oberta de Catalunya).

31

Desde el punto de vista de este autor, la dificultad surge a la hora de identificar cómo abordar esta regulación y dotar de seguridad jurídica a los distintos usos de la inteligencia artificial en las administraciones públicas, fomentando la innovación y garantizando su rápida adaptación.

La solución pasa, en su opinión, por la aplicación de las herramientas metodológicas generadas para la regulación de Internet por autores como Calo (2016:112), reconociendo la oportunidad de abordar la normativa a partir de la unión de los aspectos técnicos con los jurídicos, así como identificar el valor de la propia tecnología como instrumento de regulación.

En consecuencia, la inteligencia artificial está regulada en primera instancia por el código, por lo que el propio diseño o programación de algoritmos regulará su alcance. Por tanto, la pregunta, en este sentido, es si debemos considerar el código de un algoritmo una norma jurídica.

Los principales inconvenientes que Cerrillo i Martínez (2019:65) destaca para considerar estos códigos de algoritmo normas jurídicas son los relativos a que el procedimiento de elaboración de algoritmos dista mucho de cumplir con los trámites propios del procedimiento de elaboración de los reglamentos y, en particular, su publicación. Además, algunos de ellos, específicamente los que utilizan el aprendizaje automático, pueden llegar a innovar el ordenamiento jurídico al incorporar criterios que no estén explícitamente previstos en la norma.

Da este autor por buena la solución propuesta por Guihot *et al* (2017:385) de recurrir a nuevos instrumentos regulatorios como entornos supervisados para aplicar experimentalmente la regulación (*regulatory sandboxes*) donde se pueda experimentar a pequeña escala y de manera empírica con nuevos instrumentos de regulación; utilizar cláusulas derogatorias (*sunset clauses*) que permitan ir ajustando las regulaciones a la evolución tecnológica o técnicas de regulación anticipada (*anticipatory rulemaking techniques*).

32

Todo ello sin olvidar la utilidad de recurrir a la ética para regular determinados aspectos relativos a la inteligencia artificial, tal como ha hecho el Parlamento Europeo en su Resolución de 16 de febrero de 2017. En este mismo sentido, debemos tener en cuenta las Directrices éticas para una Inteligencia artificial fiable (2019), redactado por el Grupo de expertos de alto nivel sobre inteligencia artificial (IA) o la reciente Recomendación sobre la Ética de la Inteligencia Artificial (2021), aprobada por la UNESCO.

En este sentido, el enfoque se centra en garantizar el antropocentrismo, de forma que los valores humanos sean la principal consideración, siendo la IA un medio al servicio de los ciudadanos.

Desde el punto de vista del Derecho administrativo, uno de los grandes riesgos identificados por Cerrillo i Martínez (2019:62) es la existencia de sesgos, introducidos de forma voluntaria o involuntaria, o que surjan del propio aprendizaje del algoritmo a partir de datos sesgados, que pueda llevar a las administraciones públicas a adoptar decisiones discriminatorias.

Otra de las áreas de riesgo es la protección de datos personales y privacidad de las personas, en particular a través de la elaboración de perfiles o toma de decisiones automatizadas, si bien este aspecto ha sido ya abordado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos¹², que trata de poner límite a este tratamiento y reconoce a los afectados un derecho de información y acceso, además del derecho a no ser objeto de una decisión automatizada.



Por último, como se ha ido poniendo de manifiesto de forma reiterada, la transparencia como principio general de actuación de las Administraciones Públicas puede, así mismo, verse gravemente afectada por la opacidad de los algoritmos utilizados por los sistemas de IA.

2.5 Derecho procesal

El Derecho procesal no es ajeno a la evolución de la IA, en tanto en cuanto en la Administración en general y, en concreto, en la Administración de Justicia se deben implantar sistemas inteligentes, especialmente para la investigación y enjuiciamiento de los delitos.

Tanto es así, que el Anteproyecto de Ley de Enjuiciamiento Criminal aprobado el 24 de noviembre de 2020¹³, prevé la posibilidad de que el Juez de Garantías autorice la utilización de sistemas automatizados o inteligentes de tratamiento de datos para cruzar o interrelacionar la información disponible sobre la persona investigada con otros datos obrantes en otras bases de titularidad pública o privada, cuando concurren determinados requisitos.

33

La aplicación de estos sistemas en el entorno jurídico ha sido clasificada de alto riesgo por la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen las normas armonizadas sobre la Inteligencia Artificial publicado del 21 de abril de 2021 (Anexo III), en virtud de los derechos y garantías que pueden resultar menoscabados para los sujetos y para la propia Administración de Justicia.

En concreto, el Anexo enumera exhaustivamente qué casos suponen la generación de un alto riesgo en entornos jurídicos, a saber:

- a) Cuando los sistemas de IA realicen evaluaciones del riesgo sobre la reincidencia de un sujeto o sobre las víctimas de un delito.
- b) Cuando se utilicen sistemas de IA para detectar el estado emocional de una persona.
- c) Cuando los sistemas de IA se utilizan para ponderar la fiabilidad de las pruebas presentadas.
- d) Cuando los sistemas de IA sean utilizados para predecir la ocurrencia o recurrencia de un delito real o potencial, basado en la elaboración de perfiles de personas físicas o evaluar rasgos y características de la personalidad o antecedentes de comportamiento delictivo de personas físicas o grupos.
- e) Cuando dichos sistemas permitan a las autoridades policiales buscar interacciones complejas en grandes conjuntos de datos disponibles provenientes de distintas fuentes para identificar patrones desconocidos o descubrir relaciones ocultas en los datos analizados.

Frente a estos riesgos, no debemos olvidar la utilidad de la aplicación de los sistemas de IA. En opinión de Nieva Fenoll (2018: 53) en el futuro los procedimientos se sustanciarán más rápidamente y serán más previsibles en cuanto a su desarrollo, tiempo de espera y resultados, lo que permite una eficiencia necesaria en el tráfico comercial y descarga de los juzgados.

De acuerdo con San Miguel Caso (2021: 297), los sistemas de IA se convierten también en una herramienta indispensable para la configuración de estrategias procesales de defensa más eficaces que proporcionen, en función de las características del caso, datos estadísticos sobre la jurisprudencia aplicable o el perfil del juez encargado de dictar sentencia. En otro orden de cosas, también alerta la autora sobre el coste de implantación de estos sistemas y, en consecuencia, el criterio diferenciador y la indirecta desigualdad entre las partes derivada de la distinta disponibilidad de recursos.

En casos extremos podríamos llegar incluso a supuestos de indefensión en aquellos casos en que los porcentajes de éxito fueran tan limitados que llevara a los abogados a declinar la defensa del cliente.

34

Además, siguiendo a Armenta Deu (2021: 27) debemos tener en cuenta la paradoja de que la aplicación estática de decisiones dado que las bases donde se alojan los datos no son sensibles a las renovaciones sociales y jurídicas. En este mismo sentido, Barona Vilar (2019:54) habla de una merma ineludible en la capacidad decisoria del juez, cercenando el razonamiento lógico deductivo desplegado en la formulación de la sentencia.

Sobre los riesgos que esta tecnología genera en los derechos y garantías procesales de las partes en la aplicación en procedimientos judiciales de los sistemas de IA, San Miguel Caso (2021: 299) realiza una enumeración de las advertencias constantes y reiteradas realizadas desde la Unión Europea: la Comisión Europea para la Eficacia de la Justicia (2016), Carta Ética Europea sobre el uso de la Inteligencia Artificial en los sistemas judiciales y su entorno (2018), Directrices Éticas para una IA fiable del grupo de expertos independiente de alto nivel sobre IA (2018) y propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la Inteligencia Artificial (2021).

Uno de los principales problemas en el diseño de los algoritmos que utilizan los sistemas de IA son los sesgos derivados de su uso y la parcialidad del validador. Como indican Azuaje y Finol (2020:130), la objetividad de estos sistemas debe ser cuestionada desde el primer momento en el que se produce la recogida de esos datos, encontrándonos con bases de datos sesgadas por no ser una muestra aleatoria estadísticamente válida de la población de interés o porque, en algunos casos, contienen el historial de decisiones anteriores tomadas por seres humanos, basadas en los factores que se reflejan en ellas.



Además, siguiendo a San Miguel Caso (2021: 290), en aquellos supuestos en que los sistemas de IA desarrollan aprendizaje autónomo, corremos el riesgo de que al superar las barreras de la programación previa resulten indescifrables para el ser humano, de forma que la opacidad de los algoritmos represente un obstáculo generando una lesión irreversible en el derecho de defensa y una quiebra de un derecho fundamental ya que se produce un menoscabo de la tutela judicial efectiva al situar al perjudicado en una clara situación de indefensión, incumbiendo este desconocimiento también al abogado y al propio juez, hasta tal punto que será necesario que el fabricante de la herramienta desclasifique la información ya que, de lo contrario, no podrá ser utilizada la aplicación en el ámbito procesal.

En consecuencia, resulta imprescindible contar con garantías regulatorias aplicables a estos sistemas de IA, pasando la solución por la creación de sistemas diseñados con algoritmos públicos que permitieran conocer los detalles del sistema y los parámetros escogidos en la elaboración del algoritmo, en virtud del principio de transparencia algorítmica.

2.6 Derecho del trabajo

Como hemos podido constatar, desde las primeras iniciativas tendentes a dotar de un marco jurídico a los sistemas de IA, el Derecho del trabajo es, sin duda, una de las áreas más sensibles en lo que a la evolución y regulación de los sistemas de IA se refiere. Uno de los debates cruciales a este respecto es si debería regularse un derecho del trabajador a no ser reemplazado por un software o una máquina.

De acuerdo con la OCDE, un 21% de los empleos en España están en riesgo de desaparecer o transformarse significativamente por la automatización y un 14% para el conjunto de los países de la UE. Dicha tendencia, además, se ha acelerado con la pandemia¹⁴.

Repasemos, a continuación, algunos de los pronunciamientos judiciales en España respecto de la posible sustitución de trabajadores por sistemas de IA.

En septiembre de 2019, el juzgado de lo Social número 10 de Las Palmas de Gran Canaria declaraba improcedente el despido de una administrativa por ser sustituida por un robot. La trabajadora llevaba trece años trabajando en las oficinas centrales de la compañía como oficial de contabilidad, hasta que la firma adquirió la licencia de Jidoka, un RPA (*Robotic Process Automation*) para la gestión de cobros. Esta máquina realiza tareas desde las 17.15h hasta las 6.00h en días laborales y 24 horas los festivos. Dicha automatización supuso el despido de varios trabajadores por causas productivas.

El juez consideró que dicha automatización ejecutada para reducir costes es igual a reducir el derecho al trabajo para aumentar la libertad de empresa. Además, entiende que

para justificar el despido por razones objetivas es necesario acudir a una causa excepcional, no pudiendo considerarse tal la automatización de tareas desarrolladas hasta ahora por humanos. De acuerdo con el razonamiento del juez “la automatización como causa técnica del despido objetivo implica una oposición entre los derechos sociales alcanzados por los trabajadores que se vislumbran como obstáculo para alcanzar un rendimiento empresarial óptimo, frente a la posibilidad de que un instrumento de producción pueda efectuar ese mismo trabajo sin límite de horas, sin salario ni cotizaciones sociales”.

La necesidad de innovación empresarial, reducción de costes y aumento de competitividad es obvia y completamente legítima desde el punto de vista empresarial. El problema se genera para determinar un criterio de proporcionalidad entre la adquisición de un robot y la amortización de puestos de trabajo, algo que ya apunta el artículo 52.b) del Estatuto de los Trabajadores cuando establece como causa de despido objetivo la falta de adaptación del trabajador a las modificaciones técnicas operadas en su puesto de trabajo, cuando dichos cambios sean razonables.

36

En la Conferencia de alto nivel de la UE sobre el futuro del trabajo¹⁵ los expertos inciden en el riesgo que implica la polarización y desigualdad laboral, en el sentido de que aumentará la robotización en empleos menos cualificados y con menos salarios y se mantendrán o aumentarán los empleos más cualificados y mejor retribuidos.

Dicho criterio de proporcionalidad es el utilizado por el Tribunal Superior de Justicia de Madrid en su fallo de 7 de octubre de 2019¹⁶ para declarar improcedente el despido de nueve empleados tras la adquisición de nuevas rotativas por la imprenta. De acuerdo con la sentencia, la dirección debería presentar pruebas para justificar el despido más allá de la simple mejora de la productividad. De hecho, argumentó la Sala que el aumento de volumen de producción podría llegar a implicar la necesidad de más personal, especialmente dado que la empresa recurría a ETT en determinados picos de producción para los que podía haber utilizado a los trabajadores despedidos.

Una de las posibles soluciones planteadas por Puente Pérez (2019: 43) es la posibilidad de incluir supuestos de este tipo en la negociación colectiva, garantizándose la intervención de los representantes de los trabajadores con la emisión de informes en los casos necesarios.

En cualquier caso, como afirma Bonet Pérez (2018: 4), lo que parece innegable es que la automatización y la digitalización traerán, cuanto menos, un aumento temporal del desempleo o la consolidación de un nivel de desempleo estructural significativo que genere necesidades de protección social más amplias, dado el número de personas afectadas por el proceso disruptivo.



Por este motivo la OIT propone un programa centrado en las personas para el futuro del trabajo y recomienda centrar los esfuerzos en aumentar la inversión en las capacidades de las personas, en las instituciones del trabajo y en trabajo decente y sostenible¹⁷.

En cualquier caso, hasta alcanzar dicha estabilidad, otro de los problemas que se plantea en el ámbito del Derecho de trabajo es la contribución a la financiación de los sistemas públicos de la Seguridad Social.

Como indica Puente Pérez (2019: 50), desde el punto de vista del Derecho del trabajo, actualmente no se puede plantear dicha cotización de los sistemas de IA como cualquier trabajador para contribuir a la financiación de los sistemas públicos de la Seguridad Social.

Entre otras cuestiones, el sistema de la Seguridad Social tiene por finalidad garantizar que las personas comprendidas en el campo de aplicación del Texto Refundido de la Ley General de la Seguridad Social, sus familiares o asimilados a su cargo tengan una protección adecuada frente a las contingencias u otras situaciones contempladas, siendo dichas contingencias la incapacidad, maternidad o paternidad, jubilación, etc. Es decir, estas situaciones están siempre vinculadas a las distintas circunstancias que atraviesan las personas físicas.

37

Coturel (2021: 30) nos proporciona ejemplos que van más allá de la sustitución de trabajadores por sistemas de IA y que afectan, plenamente, a la contratación y despido de trabajadores efectuadas por máquinas. En el año 2018, en EEUU se produjo el despido de un trabajador por autodeterminación del sistema informático de una empresa, ante la omisión de la carga de datos del superior del trabajador. También se hizo pública la información de que, en 2014, Amazon desarrolló un sistema de Inteligencia Artificial para seleccionar candidatos a empleos, que luego de varios años de desarrollo demostró que no seleccionaba mujeres y rechazaba sistemáticamente los currículums enviados por personas del género femenino.

En este sentido, el uso de la inteligencia artificial y los smart contracts puede implicar el problema de la imposibilidad de detener la auto ejecución del contrato, para lo que Coturel recomienda la existencia de un “botón de pánico” a través del cual detener dicha automatización. Además, recuerda la necesaria aplicación del artículo 22 del Reglamento General de Protección de Datos en virtud del cual toda persona tiene derecho a que una decisión final no sea tomada de forma automatizada.

2.7.Derecho mercantil

Sin lugar a ninguna duda, las diferentes manifestaciones de la IA plantean un conflicto entre el desarrollo empresarial, la información, los secretos empresariales y la privacidad y protección de datos.

Dado que las innovaciones en la transformación digital se basan en herramientas y aplicaciones sustentadas en la IA, una de las primeras cuestiones a analizar es determinar qué mecanismos jurídicos van a permitir proteger estas innovaciones.

Por una parte, se tratará de determinar qué innovaciones son patentables y si hay otros métodos de protección compatibles y, por otra, cómo se protegen los datos como fuente de riqueza empresarial para las empresas.

Ahondando en este último aspecto, debemos tener en cuenta que uno de los pilares esenciales del aprendizaje automático (*machine learning*) son los datos gracias a los cuales se desarrollan algoritmos y tecnologías que hacen posible que los ordenadores reproduzcan habilidades cognitivas similares a los seres humanos.

En este sentido, los operadores tratan de hallar fórmulas para usar dichos datos en exclusiva, preguntándose la doctrina si es posible aplicar la protección establecida por la Ley 1/2019, de 20 de febrero, de Secretos Empresariales¹⁸.

38

A este respecto, la OMPI celebró los días 25 y 26 de noviembre de 2019 un Simposio sobre Secretos Empresariales e Innovación¹⁹, habiendo observado una mayor demanda de recursos judiciales cuando los datos son objeto de utilización o apropiación indebidas en la economía digital, dado el valor creciente de dichos datos como activo comercial y científico.

El representante español en dicho Simposio, Otero Lastres, reflexionaba sobre la tercera vía que utilizan los innovadores actualmente. En la mayoría de los casos se patenta la característica técnica esencial de las invenciones, manteniendo en secreto los conocimientos en torno a la patente. Cuando el conocimiento técnico conduce a una nueva patente, se suma a la anterior.

En todo caso, la protección como secreto comercial parece plantearse como la única opción posible en determinadas situaciones como las primeras etapas de la innovación, cuando las innovaciones no pueden acogerse a la protección como patente tales como las ideas abstractas, los procedimientos o los métodos y planes comerciales o empresariales.

Se plantea, así mismo, la posibilidad de registrar los secretos comerciales ante una entidad de confianza para resolver los problemas que plantea demostrar su existencia y titularidad, utilizando soluciones basadas en las cadenas de bloques, que pueden proporcionar un registro de tiempo, inmutable y rastreable, e incluso el contenido del secreto comercial, garantizando que los secretos comerciales no puedan piratearse ni ponerse a disposición de terceros.



Como afirma De La Quadra Salcedo (2018: 23), quien dispone de los datos junto con el conocimiento y las técnicas para trabajarlos está en una situación de ventaja competitiva que puede distorsionar la libre competencia, pilar fundamental para el correcto funcionamiento de los mercados. Por lo tanto, es necesario analizar la patentabilidad de los sistemas de IA.

Fernández Pérez (2021: 78) distingue tres tipos de patentes:

- a) Patentes en materia de hardware, software y conectividad, que permiten transformar cualquier objeto en un dispositivo inteligente conectado a través de Internet y que son la base del Internet de las cosas IoT.
- b) Patentes relativas a invenciones relacionadas con la seguridad, análisis de datos, IA, sistemas 3D e interfaces de usuario, que se usan en combinación con objetos.
- c) Patentes relacionadas con procesos de fabricación, infraestructuras (ciudades inteligentes), transportes (coches autónomos) o personas (monitorización de enfermedades)

Es en el caso de este último tipo de patentes donde Fernández Pérez (2021: 81) plantea interrogantes de cara a su patentabilidad, en tanto en cuanto en el caso de las invenciones implementadas en ordenador destaca el riesgo, en el caso de una eventual ausencia de carácter técnico, de la exclusión del concepto de invención y, por tanto, de patentabilidad.

39

Nos recuerda esta autora como, a lo largo de los años, la Oficina Europea de Patentes (EPO) ha ido aclarando el artículo 52 de la Ley de Patentes, determinando que es preciso un “efecto técnico” como puede ser que bajo la influencia del programa informático se logre el control de la ejecución del programa, como hace también la Oficina Española de Patentes y Marcas (OEPM) en casos como dispositivos médicos, programas de traducción automática de lenguaje natural, etc.

En cualquier caso, tanto la complejidad de las invenciones como el hecho de que partan de programas y aplicaciones informáticas plantea la necesidad de analizar caso por caso, desde el punto de vista jurídico, estas invenciones.

2.8.Responsabilidad civil

Como indica Gómez-Riesco (2019: 123), lo que subyace a todas las posibles soluciones es la necesidad de lograr el equilibrio entre la exigencia de resarcimiento por los daños que puedan sufrir las víctimas por la acción de los robots y la conveniencia de fomentar el desarrollo de los sistemas de IA por las ventajas que pueden generarse para la sociedad.

En el ámbito de la responsabilidad civil, Gómez-Riesco (2019: 129) analiza si ante la posibilidad del mayor o menor grado de autonomía e inteligencia del robot, podríamos llegar a tratar la responsabilidad civil por los daños que se originen por su actuación desde un punto de vista distinto al del régimen de responsabilidad civil por daños causados al

consumidor y por productos defectuosos. El problema de plantear una nueva regulación son las posibilidades de desarrollo e innovación que, actualmente, resultan impredecibles.

Sin embargo, dada la inseguridad jurídica que genera la falta de regulación, así como el esfuerzo jurisprudencial que implicaría dar solución a los problemas de responsabilidad civil que se planteen por estas nuevas realidades, sí es necesario un marco jurídico propio que dé respuesta a los problemas en el uso de los sistemas de IA en el tráfico.

Una solución, propone este autor, podría ser establecer un sistema de responsabilidad objetiva o de gestión de riesgos que obligue a reparar el daño causado por los robots, por el mero hecho de haberse ocasionado tales daños, y estableciendo un seguro obligatorio para cubrir los posibles daños. Para ello se puede partir de supuestos especiales en los que la legislación ha establecido mecanismos de responsabilidad civil objetiva o cuasiobjetiva de forma que, por la creación del riesgo y daño potencial, se obliga a responder al fabricante o propietario en el supuesto de que efectivamente se materialice el daño. Todo ello teniendo en cuenta que no se debe llegar a situaciones en las que los fabricantes de robots desistan de seguir desarrollando nuevos sistemas si las responsabilidades pueden ser imprevisibles y excesivas, disminuyéndose la innovación e, incluso, negándose las compañías a asegurar dichos riesgos.

40

El Parlamento Europeo dictó una Resolución el 20 de octubre de 2020, sobre el Régimen de responsabilidad civil en materia de inteligencia artificial²⁰, acompañada de un Anexo con *“recomendaciones detalladas para la elaboración de un Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial”*.

Una de las mayores preocupaciones del Parlamento es la imposibilidad de determinar, en la utilización de determinados sistemas de IA, quién controlaba el riesgo asociado al sistema de IA o qué ha provocado, en última instancia, el funcionamiento lesivo, lo que podría dificultar la identificación de la relación entre el daño o perjuicio y el comportamiento que lo causa, con el resultado de que las víctimas podrían no recibir la indemnización adecuada.

En cualquier caso, el Parlamento considera que no es necesaria una revisión completa de los regímenes de responsabilidad civil que funcionan bien, si bien sí es necesario adecuarlo dada la complejidad, conectividad, opacidad, vulnerabilidad, modificación mediante actualizaciones, autoaprendizaje y autonomía potencial de los sistemas de IA, así como la multitud de agentes involucrados.

Ciertos obstáculos se podrían eludir haciendo responsables a las diferentes personas de toda la cadena de valor que crea, mantiene o controla el riesgo asociado al sistema de IA.



El Parlamento Europeo, junto con el seguro obligatorio, plantea la creación de un fondo de compensación que garantice la reparación de los daños o perjuicios causados ante la ausencia de un seguro o dónde éste no alcance.

2.9.Derecho penal

En el ámbito del Derecho Penal nos encontramos ante una encrucijada quizás aún más compleja. Como señala Domínguez Peco (2019: 156), los problemas de la regulación legal de los sistemas de IA pueden abordarse de dos maneras: desde un punto de vista parcial y práctico, analizando cómo deben operar las reglas del derecho vigente; o proponiendo la creación de un *corpus* propio, lo que requiere como presupuesto el reconocimiento a los robots de una cierta entidad como sujetos de Derecho. En este sentido, señala la autora que el importante antecedente que supone la atribución de responsabilidad a las personas jurídicas. En este sentido, el elemento de culpabilidad recogido en el Código Penal (*no hay pena sin dolo o imprudencia*) impide una traslación directa de las leyes penales a la robótica, dado el estado actual de la ciencia.

Cuestión diferente, señala esta autora, es la responsabilidad relacionada con la comisión de delitos a través de los robots. Siguiendo la doctrina penalista, si el autor mediano es quien emplea a la persona ejecutante como si fuera un mero instrumento, existe la posibilidad de aplicar a los casos de utilización de robots esta teoría. El problema, indica Domínguez Peco (2019: 158), es que no resulta posible su aplicación en tanto en cuanto los robots mantienen la configuración y el tratamiento jurídico de las cosas.

41

En tanto que el robot es una herramienta, las consecuencias de las acciones serán imputables a quien lo controla, siempre que concurra imprudencia o dolo en su uso.

El pasado 6 de octubre de 2021 el Parlamento Europeo dictó una Resolución sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales²¹.

En este caso se trata de analizar qué sistemas de IA se están utilizando, o es previsible que se utilicen, por las autoridades policiales y judiciales y qué medidas de prevención considera necesarias el Parlamento para asegurar los derechos de los ciudadanos, todo ello partiendo de la base de la normativa existente en la UE en cuanto a protección de la vida privada y los datos de carácter personal.

Dadas las consecuencias que tiene la utilización de sistemas de IA para la vida de las personas, el Parlamento considera que toda herramienta de IA desarrollada o utilizada por las autoridades policiales o judiciales debe, como mínimo, ser segura, robusta, fiable y apta para su finalidad, así como respetar los principios de minimización de datos, rendición de cuentas, transparencia, no discriminación y explicabilidad, y que su

desarrollo, despliegue y uso deben estar sujetos a una evaluación de riesgos y a una estricta comprobación de los criterios de necesidad y proporcionalidad.

A este respecto, aclara que la vigilancia masiva mediante tecnologías de IA, por definición, no cumple los principios de necesidad y proporcionalidad, por lo que considera esencial prohibir el uso de aplicaciones que puedan dar lugar a dicha vigilancia masiva.

En cuanto a la identificación individualizada, destaca que muchas tecnologías de identificación basadas en algoritmos utilizadas actualmente identifican y clasifican incorrectamente en un número desproporcionado de casos a las personas racializadas, a las personas pertenecientes a determinadas comunidades étnicas, a las personas LGBTI, a los niños y a las personas de edad avanzada, así como a las mujeres.

Ante la dificultad de atribución de responsabilidad individualizada por posibles daños, subraya que la responsabilidad legal debe recaer siempre en una persona física o jurídica, que siempre debe estar identificada en el caso de las decisiones adoptadas con el apoyo de la IA. Por lo tanto, es necesario garantizar la transparencia de las estructuras empresariales que producen y gestionan sistemas de IA.

42

Uno de los problemas esenciales a este respecto es la imposibilidad de elaborar una lista exhaustiva de aplicaciones, por lo que considera imprescindible un modelo de gobernanza claro y coherente que garantice tanto los derechos fundamentales de las personas como claridad jurídica para los desarrolladores, siguiendo los cinco principios de la Carta Ética sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno adoptados por la CEPEJ (Europe European Commission for the efficiency of Justice)²².

Partiendo de la situación actual de la tecnología, solicita la prohibición permanente del uso de análisis automatizados o el reconocimiento en espacios accesibles al público de características humanas, y pide una moratoria al despliegue de sistemas de reconocimiento facial para fines coercitivos con funciones de identificación, salvo que sean utilizados estrictamente para fines de identificación de víctimas de delitos, hasta que las normas técnicas puedan considerarse plenamente acordes con los derechos fundamentales.

Incluye la Resolución un tema de estricta actualidad, como el de la utilización por parte de las fuerzas del orden y los servicios de inteligencia de bases de datos de reconocimiento facial privadas, como Clearview AI, con más de 3.000 millones de imágenes recopiladas de Internet.

En este caso concreto, el Parlamento pide a los Estados miembros que obliguen a los agentes a revelar si están utilizando esta tecnología, o la de otros proveedores, dado que



en opinión del Comité Europeo de Protección de Datos es uso de este servicio probablemente no sería compatible con el régimen de protección de datos de la UE.

No solo muestra el Parlamento su preocupación por estos proyectos, sino también por aquellos financiados en el marco de Horizonte 2020 que implantan inteligencia artificial en fronteras exteriores, como el proyecto iBorderCtrl, que elabora perfiles de los viajeros partiendo de una entrevista automatizada por ordenador a través de la cámara web del viajero y un análisis de microgestos.

Este proyecto ha sido probado en Hungría, Letonia y Grecia y el Parlamento solicita en este caso a la Comisión que, incluso a través de procedimientos de infracción en caso de ser necesario, aplique la prohibición de cualquier tratamiento de datos biométricos, incluidas imágenes faciales, con fines coercitivos que dé lugar a una vigilancia masiva en espacios abiertos, así como que deje de financiar proyectos de investigación biométrica o vigilancia masiva, incluyendo el uso de drones en operaciones policiales.

Sin embargo, no debemos olvidar las ventajas de la utilización de sistemas de IA por las Fuerzas y Cuerpos de seguridad como ocurre, por ejemplo, en la criminología medioambiental. Como indica Balcells (2020: 231) varias han sido las causas del cambio que ha conducido a una policía eminentemente reactiva a una de predictiva, pero una fundamental ha sido el análisis geográfico de los delitos. La criminología medioambiental enmarca una serie de teorías con un nexo común: los hechos criminales y las circunstancias inmediatas donde los delitos ocurren. El delito sucede en espacios que pueden ser predichos porque las oportunidades delictivas coinciden en zonas conocidas por el delincuente. A su vez, hay determinados espacios que se convierten en puntos calientes (*hot spots*) porque el nivel de convergencia de delincuentes y víctimas es muy elevado, y, por lo tanto, las oportunidades se disparan.

43

Estamos de acuerdo con Martínez Martínez (2019: 70) cuando afirma que, sin alarmismos, pero sí con cautelas, lo aconsejable es que el legislador opte por avanzar en el camino de los sistemas de IA progresivamente, primero centrando sus esfuerzos en herramientas predictivas complementarias y, posteriormente, avanzar en la sistematización de operaciones con cierto grado de autonomía.

2.10. Derecho tributario

Desde el punto de vista del Derecho Tributario se han barajado opciones tendentes a establecer una fiscalidad específica para los sistemas de IA.

Debemos recordar que la idea de crear un marco jurídico europeo tiene como finalidad incentivar la investigación e implantación de nuevos sistemas de IA con la finalidad de que la UE se convierta en líder en este ámbito. Sin embargo, si se grava la introducción de sistemas de IA en la actividad para mejorar la productividad, necesariamente se

desincentivaré la apuesta por estos sistemas. Además, como apunta Segura Alastrué (2019: 85), desde un punto de vista de técnica tributaria se plantean problemas tanto desde el punto de visto de determinar de forma absolutamente clara tanto el hecho y base imponible, como el sujeto pasivo. No es fácil reconocer qué tecnologías son sustitutivas de los humanos y, en la mayoría de los casos, estamos hablando de un software. Además, las empresas pasarían de considerar las inversiones tecnológicas un activo deducible, a un bien que genera una tributación adicional.

También genera dudas si la renta que generase el robot se gravaría en el ámbito de la tributación sobre las personas jurídicas o si se trasladaría al IRPF, así como la magnitud sobre la que debería recaer la base imponible del impuesto, esto es, la productividad de la máquina, el salario que considerara la empresa que podría recibir el robot, etc.

En opinión de este autor, la idea de compensar a los ciudadanos que se queden sin empleo por la introducción de los sistemas de IA a través de una renta básica universal es desafortunada, por los perniciosos efectos que conlleva. Como él explica, la renta básica es una ayuda incondicional, con independencia del nivel de ingresos del receptor, lo que se desconoce qué efectos puede tener en el comportamiento de las personas. El presupuesto necesario para mantenerlo sería tal que devendría inasumible.

A pesar del interés de centrar el debate en la posible personalidad electrónica de los robots, parece claro que con el estado actual de las cosas no es fructífero ahondar en más allá en él, sino más bien analizar desde un punto de vista descriptivo qué instrumentos jurídicos se están desarrollando en el ámbito de la UE para dotar de regulación a los sistemas actuales sin disminuir la inversión en IA y, en consecuencia, la innovación en este ámbito, a la vez que se dota a los usuarios de la confianza suficiente en estos sistemas para incrementar su adopción.

3. LOS PILARES DEL LIBRO BLANCO

Una vez planteado el problema, determinaremos la base para el desarrollo de los sistemas de IA en la UE, establecidos por el Libro Blanco sobre inteligencia artificial, un enfoque europeo orientado a la excelencia y confianza, anteriormente citado.

El Libro Blanco parte de la oportunidad que supone para Europa, dada su estrecha vinculación con los valores y el estado de Derecho, de generar confianza en las personas que van a tener presente la tecnología digital en todos los aspectos primordiales de su vida. Por ello, todo desarrollo de la IA en la sociedad debe estar asentado en la dignidad humana y la protección de la privacidad junto con la consecución de los Objetivos de Desarrollo Sostenible.



Partiendo de esta base, los pilares del Libro Blanco son los siguientes:

- **Ecosistema de excelencia:** el marco político debe establecer medidas para armonizar los esfuerzos regionales, nacionales y europeos, en colaboración con los sectores público y privado, a lo largo de toda la cadena de valor.
- **Ecosistema de confianza:** la base para el desarrollo de la IA debe ser la protección de los derechos fundamentales y los derechos de los consumidores, especialmente con relación a aquellos que presentan un riesgo elevado.

Todo ello partiendo de la base de que la Comisión respalda un **enfoque antropocéntrico** tal como explicita en la Comunicación *Generar confianza en la inteligencia artificial centrada en el ser humano*²³. No podemos olvidar que el Libro Blanco viene acompañado por la Estrategia Europea de Datos²⁴ que busca convertir la UE en líder de una sociedad impulsada por los datos. Un primer paso en este sentido es la creación de un mercado único de datos en la UE en beneficio de empresas, investigadores y administraciones públicas, teniendo en cuenta que los datos son esenciales para la transformación digital y, en consecuencia, para la innovación y el crecimiento.

Lo esencial a este respecto es que, en paralelo con la libre circulación de datos no personales, se respeten las normas europeas de privacidad, protección de datos y competencia, así como que las normas para el acceso a los datos y su utilización sean justas y claras.

45

En la UE es constante la idea de la necesidad de liderar una transformación digital que esté basada en tres pilares:

- **La tecnología al servicio de las personas:** el liderazgo en la transformación digital debe venir acompañado de inversiones en competencias digitales para los ciudadanos, protegiéndoles contra las amenazas cibernéticas y con un desarrollo de la IA respetuoso con los derechos de las personas y en la que puedan confiar.
- **Una economía digital justa y competitiva:** reforzando la responsabilidad de las plataformas online al proponer una ley de servicios digitales y clarificar las normas sobre servicios online, garantizando la protección de los datos personales y sensibles y garantizando la adecuación de las normas de la UE para la economía digital.
- **Una sociedad abierta, democrática y sostenible:** este pilar recoge distintas metas, desde el compromiso de que Europa llegue a ser climáticamente neutra en 2050, hasta la lucha contra la desinformación online o la creación de un “espacio europeo de datos de salud” para favorecer la investigación, el diagnóstico y el tratamiento específicos.

Desde el cumplimiento de estos pilares, la estrategia digital de la UE se diseña como una herramienta beneficiosa para los ciudadanos europeos, poniendo la tecnología al servicio de su vida cotidiana; para las empresas, al capacitarlas para nacer, crecer, innovar y competir en condiciones justas; y, finalmente, para el medio ambiente, al lograr la neutralidad climática con la ayuda de las tecnologías digitales.

Algunos ejemplos de utilización de datos de industrias para una mejor asignación de recursos indican, por ejemplo, que la navegación en tiempo real para evitar el tráfico puede ahorrar hasta 730 millones de horas, lo que implica 20.000 millones de euros en costes laborales, o que la notificación en tiempo real de los trenes con retraso puede ahorrar 27 millones de horas de trabajo, lo que representa hasta 740 millones de euros de costes laborales¹².

Uno de los puntos clave a este respecto es la necesidad de que la UE sea creadora y productora de la tecnología en IA, teniendo en cuenta su capacidad industrial en sistemas digitales seguros y protegidos de bajo consumo de energía o el volumen de datos públicos y de la industria con los que cuenta.

46

El reto ante el que se encuentra la UE es aprovechar esa capacidad para reforzar su soberanía tecnológica y materializar una IA basada en los valores y normas europeos. Si tenemos en cuenta la evolución de la financiación en investigación e innovación en IA desde 2016 hasta 2019, el aumento es de 1.500 millones de euros, lo que supone un incremento del 70% en comparación con el periodo anterior. Aún así, valores alejados de la inversión en Asia o América del Norte (McKinsey, 2017).

Para ello la UE viene desarrollando el Plan Coordinado sobre IA, iniciado en 2018, y cuya última actualización es de 21 de abril de 2021¹³. Este último Plan Coordinado implica un conjunto de acciones y reglamentos para gestionar el desarrollo de la IA en la UE. Es un compromiso conjunto emitido por la Comisión Europea y los Estados miembros, ampliando el de 2018, en el sentido de que no solo se entra en la maximización de las inversiones a la IA y la previsión del marco para operar, sino que, si bien su foco sigue siendo permitir la IA, examina sus riesgos desde el punto de vista de la seguridad, la ética, el uso público, la innovación y el clima y el medio ambiente.

En definitiva, la revisión del Plan Coordinado y su actualización en 2021 son reflejo de la visión de que, para tener éxito en el liderazgo mundial de una IA de confianza, es necesario que la Comisión Europea, los Estados miembros y actores privados lleven a cabo las siguientes acciones:

- acelerar la investigación en tecnologías de IA para impulsar una recuperación económica y social resiliente, facilitada por la adopción de nuevas soluciones digitales;



¿Estamos caminando hacia el reconocimiento de la personalidad jurídica a los robots en la Unión Europea?

- actuar sobre las estrategias y programas de IA, implementándolos de manera completa y oportuna, garantizando que la UE obtenga todos los beneficios de las ventajas de ser los pioneros; y
- alinear la política de IA para eliminar la fragmentación y abordar los desafíos globales.

Existen varios programas para acelerar las inversiones públicas y privadas, aprovechando la financiación disponible de la UE como, por ejemplo, *Digital Europe (DEP)*²⁷, *Horizon Europe (HE)*²⁸ o *Recovery and Resilience Facility (RRF)*²⁹.

Desde el punto de vista de la inversión, la propuesta de la Comisión es que la UE invierta al menos 1 billón de euros al año en los programas *HE* y *DEP* en el periodo 2021-2027. Por su parte, el *RRF* es el paquete de estímulo más grande que ha financiado el presupuesto de la UE, proporcionando a los Estados miembros apoyo anticipado en forma de préstamos y subvenciones de 672.500 millones de euros para los años iniciales de la recuperación, proponiéndose el 20% de esta financiación para el objetivo digital.

El Programa Europa Digital proporciona financiación para proyectos en cinco ámbitos:

- Supercomputación,
- Inteligencia artificial,
- Ciberseguridad,
- Competencias digitales avanzadas, y
- Generalización del uso de las tecnologías digitales en todos los sectores de la economía y la sociedad.

Una de las preocupaciones de la UE es la brecha entre la investigación de la tecnología digital y la implantación en el mercado, teniendo como objetivo este programa estrechar esta brecha.

Por su parte, el Programa Horizonte Europa es el instrumento para llevar a cabo las políticas de I+D+I de la UE con el objetivo de que las inversiones de la UE en I+D alcancen un impacto científico, tecnológico, económico y social, fortaleciendo sus bases científicas y tecnológicas y fomentando la competitividad de todos los Estados Miembros.

El tercer pilar de este proyecto, Europa Innovadora, se dirige nuevamente al objetivo de hacer de Europa una potencia pionera en la innovación de creación de mercado y en el crecimiento de pymes innovadoras a través del Consejo Europeo de Innovación (EIC), con la ambición de crecer a escala internacional y con el fomento de la integración de la investigación, la educación superior y el emprendimiento a través de las Comunicaciones de conocimiento e innovación (KIC) que desarrolla el Instituto Europeo de Innovación y Tecnología (EIT).

Los dos pilares adicionales de este programa son: Ciencia Excelente, dedicada a financiar proyectos de investigación a través del Consejo Europeo de Investigación (ERC); y Desafíos Globales y Competitividad Industrial Europea, que financia la investigación dentro de los retos sociales y apoya la creación de asociaciones europeas con los Estados Miembros y la industria para trabajar en I+I, junto con el Centro Común de Investigación (JRC).

Estos pilares se sustentan sobre un programa horizontal, ERA (Ampliando la participación y fortaleciendo el Área Europea de Investigación) dedicado a ayudar a los Estados Miembros en el desarrollo de su potencial nacional de investigación e innovación, en especial a aquellos con un menor rendimiento en I+I.

Por último, el objetivo del *RRF* es apoyar las reformas e inversiones emprendidas por los Estados Miembros para mitigar el impacto social y económico de la pandemia y hacer que las economías y sociedades europeas sean más sostenibles, resilientes y estén mejor preparadas para la transición verde y la digital.

48

Dada la necesidad de la actuación en estos ámbitos, para beneficiarse del apoyo de este mecanismo las reformas e inversiones deben implementarse para 2026 y los planes deben abordar eficazmente los desafíos identificados en el Semestre Europeo. Por otra parte, cada plan debe contribuir a las cuatro dimensiones descritas en la Estrategia anual de crecimiento sostenible de 2021, que lanzó el ciclo del Semestre Europeo de este año:

- Sostenibilidad del medio ambiente,
- Productividad,
- Justicia, y
- Estabilidad macroeconómica

El contexto de estos programas viene determinado por los cambios en el valor y la reutilización de los datos en los distintos sectores. El volumen de datos producido en el mundo, según predicciones de IDC, pasará de 33 zetabytes en 2018 a una previsión de 175 zetabytes en 2025 (IDC, 2019)³⁰, suponiendo esta nueva oleada de datos una oportunidad para que Europa se posicione en la economía ágil en el manejo de datos. A ello hay que sumarle el cambio previsto en la manera en la que se tratarán los datos siendo que el porcentaje del 80/20 de tratamiento de datos en la nube de centros de datos centralizados frente al de aparatos inteligentes conectados e instalaciones informáticas cercanas al usuario (*edge computing*) está previsto que de aquí a 2025 cambie de manera notable (Gartner, 2017)³¹.

Uno de los elementos clave en la automatización de los procesos industriales (industria 4.0) y modos de transporte, es el liderazgo de Europa en soluciones neuromórficas, es decir, aquellos sistemas de gran escala compuestos por circuitos integrados que imitan la arquitectura neuronal biológica³².



Martínez de Pisón (2017:65) recuerda las predicciones de Kurzweil en este sentido: “En una primera fase, que se materializaría a finales de la década de 2020, la ciencia habrá completado el proceso de aplicación de la ingeniería inversa del cerebro, de manera que tendremos un mapa que permitirá crear sistemas no biológicos que cumplan con los patrones de inteligencia, incluida la emocional. La siguiente fase permitirá cargar los datos del cerebro biológico -conocimiento, conciencia, experiencia, etc.- en un sustrato no biológico pensante adecuado para ello. En un tercer momento, el más emocionante de todos, supondrá el paso de lo biológico a lo no biológico. Esto ya ha comenzado con la benigna introducción de dispositivos tales como implantes neuronales. Se harán progresos con la introducción de nanorobots en el torrente sanguíneo. Más tarde, nanorobots más sofisticados harán de interfaces con nuestras neuronas biológicas para mejorar nuestros sentidos, proporcionando con ello realidad virtual y aumentada. También ayudarán a nuestra memoria y realizarán otras tareas cognitivas rutinarias. Entonces seremos cyborgs. Todo ello se materializará en la década de 2040, en la que la parte no biológica será más potente que la biológica”.

En este estado de las cosas, la Comisión considera que se dan las condiciones para crear un ecosistema de excelencia, si bien es necesario reforzar acciones en distintos niveles, como veremos a continuación.

49

Como anteriormente expusimos, el fomento del desarrollo y utilización de la IA en Europa proviene de la Estrategia sobre la Inteligencia Artificial de abril de 2018³³ y el Plan Coordinado³⁴ de ese mismo año, preparado con los Estados Miembros. En cuanto a la colaboración con los Estados Miembros, la Comisión consideró necesario revisar el Plan Coordinado, una vez se contara con los resultados de la consulta pública sobre el Libro Blanco, revisión que dio lugar al Plan Coordinado 2021 anteriormente citado.

Además, la Comisión considera esencial la creación de centros de excelencia y pruebas de referencia mundial para combinar inversiones europeas, nacionales y privadas en el marco de los programas *DEP* y *HE*.

Para ello es necesario, además, contar con redes de universidades y centros de educación superior pioneros, para atraer a los mejores científicos y ofrecer programas de máster de IA situados a la vanguardia mundial.

El programa Europa Digital es también clave para garantizar el objetivo de la cooperación entre pymes y, en concreto, la plataforma “inteligencia artificial a la carta”³⁵ y el programa InvestEU³⁶. En este sentido, cada Estado miembro deberá contar un centro de innovación digital con un elevado nivel de especialización en inteligencia artificial, respaldados por el Programa Digital Europeo.

También es necesaria la plena participación del sector privado, así como su coinversión a través de una asociación público-privada, en el marco de *HE*, y la adopción de productos y servicios basados en la IA en Administraciones Públicas, hospitales, servicios públicos y de transporte o servicios financieros.

En definitiva, estamos hablando de que Europa se posicione en primera línea de la transformación en materia de datos e inteligencia artificial, promoviendo prácticas de gestión responsable de los datos e incentivando el cumplimiento de los principios FAIR, lo que contribuirá a generar confianza, así como a posibilitar su reutilización³⁷. De hecho, los valores compartidos de la UE y su promoción del uso ético de la IA han tenido ya influencia a nivel internacional, colaborando la UE en la elaboración de los principios éticos de la OCDE en materia de IA³⁸, principios que han sido suscritos por el G20 en su Declaración Ministerial sobre Comercio y Economía Digital de junio de 2019.

Esta labor se desarrolla igualmente en foros multilaterales, como el Consejo de Europa, la UIT o la UNESCO, tal como hemos visto anteriormente.

50

4. EL MARCO REGULADOR DE LA IA

Las expectativas de empresas y ciudadanos en cuanto al desarrollo de IA se basan en la seguridad de las primeras y la confianza de los segundos; si bien el temor al uso malintencionado de la IA y la falta de inversión o habilidades pueden constituir graves obstáculos para un desarrollo real y una adopción amplia de la IA.

En este artículo hemos revisado la estrategia destinada a aumentar la inversión en investigación, innovación y capacidad en materia de IA en la UE, pero, junto a ella, la Comisión también ha abordado los aspectos sociales creando un grupo de expertos de alto nivel que en abril de 2019 publicó directrices para una IA fiable³⁹ y que llevó a la Comisión a publicar una Comunicación acogiendo los siete requisitos esenciales contemplados en las directrices de dicho grupo⁴⁰.

Consideramos adecuado reproducir dichos requisitos, en tanto en cuanto deberán ser tenidos en cuenta para el desarrollo de las bases del Reglamento sobre el uso de la IA que posteriormente analizaremos.

- a) Acción y supervisión humanas;
- b) solidez técnica y seguridad;
- c) gestión de la privacidad y de los datos;
- d) transparencia;
- e) diversidad, no discriminación y equidad;
- f) bienestar social y medioambiental; y
- g) rendición de cuentas.



Una de las cuestiones más relevantes en cuanto a esta lista es la inclusión de tres requisitos que no son comunes en las legislaciones nacionales, a saber, transparencia, seguimiento y supervisión humana.

El mayor problema al que se enfrenta la futura legislación es que los ciudadanos exigimos un mismo nivel de seguridad y respeto de nuestros derechos, con independencia de si un sistema está o no basado en IA.

Derechos ya consolidados como la privacidad, la protección de datos, las normas de seguridad y responsabilidad civil o la no discriminación no pueden verse amenazados por la opacidad de muchos sistemas desarrollados con IA.

Por otra parte, la rapidez con la que evoluciona la IA requiere que el marco regulador deje margen para desarrollos futuros. Y, por su parte, los Estados miembros requieren un marco común europeo ya que en caso contrario existiría un riesgo cierto de fragmentación del mercado interior, lo que podría en peligro tanto los objetivos de confianza y seguridad jurídica, como el de la adopción de la IA en el mercado.

51

En este orden de cosas, los principales riesgos detectados por la UE son los siguientes:

- Riesgos para los derechos fundamentales, especialmente la protección de los datos personales y de la privacidad y la no discriminación, y
- Riesgos para la seguridad y el funcionamiento eficaz del régimen de responsabilidad civil.

Una de las preocupaciones de la UE es la relativa a la posibilidad de utilizar la IA para la vigilancia masiva de los ciudadanos en general, o los empleados de una empresa en particular. Puede ser que el uso de determinados algoritmos de IA pueda predecir reincidencia delictiva, dando lugar a prejuicios raciales o de género, hombres y mujeres, nacionales y extranjeros, etc. La complejidad y el comportamiento parcialmente autónomo de la IA puede, en este contexto, hacer difícil comprobar el cumplimiento de la legislación vigente sobre la protección de los derechos fundamentales.

Por otra parte, el uso de la IA también puede agravar los riesgos de seguridad para los usuarios cuando esté integrada en productos y servicios. En este sentido, la falta de disposiciones claras sobre seguridad puede crear inseguridad jurídica en las empresas que comercializan productos que utilicen IA en la UE.

La Comisión utiliza un ejemplo muy claro en este caso, analizando posibles problemas de aplicabilidad de la Directiva sobre responsabilidad por los daños causados por productos defectuosos dada la dificultad de demostrar, por ejemplo, la existencia de un defecto en el producto, el daño que ha generado y el nexo causal entre ambos, o la propia

aplicabilidad de la Directiva en casos, por ejemplo, en que el defecto se deba a un fallo en la ciberseguridad del producto.

En consecuencia, es claro que la legislación de la UE resulta plenamente aplicable independientemente del uso de la IA, pero la Comisión considera necesario mejorar el marco normativo para abordar los riesgos y situaciones siguientes:

- *Aplicación y ejecución efectivas de la legislación nacional y de la UE en vigor:* la preocupación viene determinada por la opacidad de la IA y, en consecuencia, la dificultad de detectar y demostrar posibles incumplimientos de la legislación, especialmente la relativa a los derechos fundamentales, imputación de responsabilidad y reclamación de una indemnización.
- *Limitaciones del ámbito de aplicación de la legislación existente en la UE:* salvo en el caso de aquellos sectores que cuentan con normativa específica, existe la duda de si un programa informático se rige por la legislación de seguridad de los productos de la UE.

La legislación general de la UE en materia de seguridad resulta de aplicación a los productos y no a los servicios y, en consecuencia, no se aplica a los servicios basados en tecnologías de IA como servicios financieros, de transporte o, incluso, servicios sanitarios.

- *Cambios en la funcionalidad de los sistemas de IA:* La incorporación de programas informáticos en los productos puede modificar su funcionamiento, lo que resulta especialmente importante en los sistemas basados en aprendizaje automático. Por lo tanto, pueden generarse nuevos riesgos inexistentes cuando se introdujo el producto en el mercado, lo que actualmente no se contempla en la legislación al centrarse fundamentalmente en los riesgos de seguridad en el momento de la comercialización.
- *Incertidumbre en lo que se refiere a la imputación de responsabilidad entre los distintos agentes económicos de la cadena de suministro:* la legislación de la UE en materia de seguridad de los productos, con carácter general, imputa la responsabilidad al productor del producto comercializado, incluidos sus componentes y, también, los sistemas de IA.

Sin embargo, estas normas son poco claras cuando el producto es comercializado por alguien que no es el productor y, por otra parte, la responsabilidad de los demás participantes en la cadena de suministro es regulada por las normas nacionales en materia de responsabilidad civil.

- *Cambios en el concepto de seguridad:* la legislación de la UE no aborda explícitamente riesgos vinculados a ciberamenazas, a seguridad personal en el



caso del uso de IA en aparatos domésticos, a la pérdida de conectividad, o al aprendizaje automático del producto cuando se está utilizando.

Los retos a los que se enfrenta el desarrollo legislativo en la UE son importantes dado que, como hemos visto, los sistemas de IA están muy lejos de haber alcanzado su desarrollo pleno y un marco normativo excesivamente rígido podría impedir su desarrollo dejando atrás los planes de liderazgo y soberanía tecnológica de la UE. Sin embargo, se parte de unos estándares legislativos en materias tales como responsabilidad civil o protección de datos que no deben verse, en ningún caso, amenazados por nuevos desarrollos.

Partiendo de estas premisas, la solución de la Comisión para abordar un marco regulador eficaz, pero no excesivamente prescriptivo, es seguir un enfoque basado en el riesgo, cuyo contenido analizaremos a continuación.

5. ENFOQUE BASADO EN EL RIESGO

53

Junto con el enfoque legislativo basado en el riesgo establecido por la Comisión, también es necesario que existan criterios claros para determinar qué aplicaciones de IA entrañan un riesgo elevado y dicha claridad y facilidad de aplicación y comprensión debe aplicar a todas las partes interesadas.

Además, debemos partir de la base de que aun cuando se considere que una aplicación de IA no entrañe un riesgo elevado debe seguir estando sujeta a la legislación de la UE.

La Comisión realiza un enfoque del riesgo basado en dos criterios:

- Que la IA se emplee en un sector en el que es previsible que existan riesgos significativos como, por ejemplo, sanidad, transporte, energía, migración, seguridad social o poder judicial, y
- Que la aplicación de IA, además, se use de manera que puedan surgir riesgos significativos. Es decir, no toda utilización de la IA en determinados sectores implica necesariamente riesgos significativos.

Solamente, por lo tanto, en el caso de que la suma de ambos criterios dé un riesgo elevado será de aplicación el nuevo marco regulador.

Puede ocurrir, sin embargo, que haya casos excepcionales en los que, debido a lo que esté en peligro, el uso de aplicaciones de IA para determinados fines se considere de elevado riesgo en sí mismo como, por ejemplo, el uso de aplicaciones de IA en procedimientos de contratación y en situaciones que repercutan en derecho de los trabajadores o aplicaciones específicas con repercusiones en los derechos de los consumidores y, también, uso de

aplicaciones para la IA para la identificación biométrica remota u otras tecnologías de vigilancia intrusiva.

Por otra parte, los requisitos para las aplicaciones de IA que entrañen un riesgo elevado pueden contar con las características clave siguientes:

- a) Datos de entrenamiento;
- b) datos y registros de datos,
- c) información a facilitar,
- d) solidez y exactitud,
- e) supervisión humana, y
- f) requisitos específicos en el caso de determinadas aplicaciones, como las empleadas para la identificación biométrica remota.

La IA depende de los datos. Sin ellos, no hay IA. Y los sistemas de IA necesitan entrenamiento y, en dicho entrenamiento, es esencial que se respeten las normas y valores de la UE relacionados con la seguridad y la legislación vigente para la protección de los derechos fundamentales. Por lo tanto, es necesario exigir el cumplimiento de determinados requisitos:

- Requisitos destinados a ofrecer garantías razonables de que el uso de los productos o servicios mediante IA es seguro, en tanto en cuanto cumple con los estándares en la normativa de seguridad de la UE como, por ejemplo, que los sistemas de IA se entrenan con conjuntos de datos suficientemente amplios y que engloban todos los escenarios pertinentes para evitar situaciones peligrosas.
- Requisitos destinados a adoptar medidas razonables para velar por que el uso posterior de los sistemas de IA no genere resultados que conlleven discriminación ilícita como, por ejemplo, la obligación de utilizar conjuntos de datos suficientemente representativos para garantizar que las dimensiones de género, etnicidad u otras de posible discriminación ilícita queden correctamente reflejadas en este conjunto de datos.
- Requisitos destinados a garantizar que la privacidad y los datos personales estén adecuadamente protegidos mientras se usen los productos y servicios basados en IA.

Otra de las cuestiones regulatorias esenciales es establecer requisitos relacionados con elementos como la complejidad y opacidad de los sistemas de IA y, en consecuencia, las dificultades para verificar de manera efectiva el cumplimiento de las normas aplicables y su ejecución.

Por lo tanto, son necesarios requisitos con relación a la conservación de registros sobre la programación de algoritmos, datos empleados para entrenar los sistemas de IA y la conservación de datos en sí mismos. Dicha información es imprescindible para el

seguimiento y comprobación de las acciones y decisiones de los sistemas de IA que pudieran ser problemáticas.

En este sentido, el marco regulatorio puede exigir la conservación de los registros exactos sobre el conjunto de datos utilizados para entrenar y probar los sistemas de IA; en determinados casos, los propios conjuntos de datos; documentación sobre metodologías de programación y entrenamiento, así como los procesos y técnicas utilizadas para probar y validar los sistemas de IA.

Más allá de los requisitos de conservación de registros, la regulación podrá establecer la necesidad de facilitar información clara sobre las capacidades y limitaciones del sistema de IA, en especial sobre el objetivo al que se destinan los sistemas, las condiciones en que deben funcionar y el nivel de exactitud esperado en la consecución del objetivo. Además, debe informarse a los ciudadanos de cuándo están interactuando con un sistema de IA y no con un ser humano y que la información proporcionada sea objetiva, concisa y claramente comprensible, adaptándose su manera de presentación al contexto específico.

La solidez, exactitud y resiliencia de los sistemas antes los ataques abiertos y los intentos de manipulación de los datos o algoritmos y las medidas para combatirlos son también esenciales. Una de las formas más eficaces para garantizar que un sistema de IA no socave la autonomía humana o provoque efectos adversos es la supervisión humana.

55

El objetivo de una IA antropocéntrica solo puede alcanzarse garantizando una participación adecuada de las personas con relación a las aplicaciones de IA de riesgo elevado y se puede traducir en consecuencias como:

- Que el resultado del sistema de IA no sea efectivo hasta que un humano no lo haya revisado y validado, o
- Que el resultado sea inmediatamente efectivo, con garantía de una intervención humana posterior.
- Que haya un seguimiento del sistema de IA mientras funciona y sea posible intervenir en tiempo real y desactivarlo.
- Que en fase de diseño se impongan restricciones operativas al sistema de IA.

Como anteriormente hemos indicado, la recopilación y uso de datos biométricos para la identificación remota entraña riesgos específicos para los derechos fundamentales. Con arreglo a la normativa vigente en materia de protección de datos, el RGPD, este tratamiento solo puede tener lugar en un número limitado de situaciones, por motivos de interés público significativo y, con arreglo a la Directiva sobre protección de datos en el ámbito penal, debe existir una autorización de la legislación nacional o de la UE y garantías adecuadas. Y todo ello debe realizarse teniendo en cuenta la aplicación de los mecanismos de evaluación de la conformidad, que existen ya en el caso de determinados productos comercializados en el mercado interior de la UE.

Cuando estos mecanismos no sean fiables, se establecerán mecanismos similares partiendo de la aportación, entre otros, de las organizaciones europeas de normalización. Una de las mayores dificultades en el caso de los sistemas que dependen de una evaluación de conformidad previa es la posibilidad de que determinados sistemas de IA evolucionen y aprendan de la experiencia, lo que requerirá evaluaciones reiteradas a lo largo del ciclo de vida de dichos sistemas.

A posteriori también será necesario mantener los controles mediante una adecuada documentación de la aplicación de IA pertinente y ofreciendo que terceros prueben dichas aplicaciones, así como ofrecer acción judicial efectiva a quienes hayan podido sufrir repercusiones negativas derivadas de los sistemas de IA.

Como indica Lacruz Mantecón (2019:27), no abarcan estas soluciones supuestos como los planteados por Navas Navarro (2017) en soluciones de IA aplicadas al Derecho como la *fuzzy logic* o lógica difusa. Estamos hablando del uso de términos lingüísticos relativos que pueden ser seguidas sin problema por un humano que es capaz de interpretar estas instrucciones rápidamente, pero difícilmente se podrán representar en un lenguaje que pueda ser entendido por un ordenador (“muy”, “lejos”, “alto”, “ligeramente”, etc). La consecuencia de estas soluciones es que generan incertidumbre en los resultados facilitados por los sistemas de IA, con el consiguiente riesgo para los afectados por sus decisiones.

Los ámbitos jurídicos en los que esta tecnología de sistemas expertos o inteligentes pueden tener aplicación en la automatización de tareas serían: análisis, extracción de información relevante, predicción, generación de argumentos, redacción de documentos contractuales, informes o memoranda, planificación de tareas en los despachos y juzgados, redacción de normas, resolución de demandas mediante técnicas automatizadas de solución alternativa de conflictos, negociación de contratos y contratación mediante programas informáticos (bots) inteligentes. Es en el caso de la contratación mediante programas informáticos donde cabe la controversia, en particular sobre si el programa negociador es un mero auxiliar o un auténtico representante del contratante. Cabe la posibilidad de que sean dos bots quienes negocien y contraten entre sí (lo que produce la desaparición del concepto de error como vicio de la voluntad).

Recuerda Lacruz Mantecón (2019: 29) otro ámbito de actuación de sistemas de IA en el Derecho, el Derecho de autor digital, en el que los interrogantes se refieren a la atribución de autoría o titularidad de creaciones exclusivamente producidas por el ordenador, en las que no se protege el resultado, sino el programa que lo produce, salvo en las legislaciones de Reino Unido, Irlanda, Nueva Zelanda o Sudáfrica, que atribuyen la titularidad a quien ha encargado la obra.



Desde nuestro punto de vista, no cabe en nuestro sistema jurídico actualmente el reconocimiento de titularidad a quien encarga la obra producida a través de un sistema de IA, quedando circunscrito el reconocimiento de la autoría al creador del sistema de IA y no al resultado creado mediante su utilización.

Por último, en el caso de las aplicaciones de IA que no consideren de elevado riesgo y no estén sujetas a los requisitos anteriormente detallados, existe la opción de establecer un sistema de etiquetado voluntario.

Mediante la utilización de la etiqueta voluntaria los agentes interesados pueden mostrar que los productos y servicios provistos de IA que ofrecen son fiables y, por su parte, los usuarios podrán distinguir fácilmente si los productos y servicios respetan referentes objetivos y normalizados, más allá de las obligaciones legales aplicables normalmente.

Obviamente, una vez que el desarrollador o implementador opte por usar este etiquetado voluntario, todos los requisitos serán vinculantes.

Por último, se requiere una estructura de gobernanza europea sobre IA en forma de un marco de cooperación de las autoridades nacionales competentes, a fin de evitar fragmentación de responsabilidades, incrementar las capacidades de los Estados miembros, y garantizar que Europa se provea a sí misma de la capacidad de probar y certificar los productos y servicios provistos de IA.

57

6. PROPUESTA DE REGLAMENTO DE LA COMISIÓN EUROPEA

Partiendo de este contexto tecnológico, social y legislativo, el pasado 21 de abril de 2021 fue publicada la versión definitiva de la propuesta de Reglamento de la Comisión Europea sobre el marco jurídico aplicable a los sistemas de inteligencia artificial, a la que hemos hecho referencia al inicio del artículo.

Por primera vez en la historia se dicta un marco jurídico sobre la IA, junto con un plan coordinado con los Estados miembros para garantizar la seguridad y los derechos fundamentales de las personas y empresas, a la vez que pretende reforzar la adopción, inversión e innovación en materia de IA en toda la UE.

Recordemos que los pioneros de la cibernética como Wiener N. (1969: 47) advertía en los años 50 de los riesgos de la nueva revolución industrial en el sentido de que podrá utilizarse en beneficio de la humanidad solo si sobrevive tanto tiempo como para llegar a un periodo en que sus ventajas sean posibles. “También podrá utilizarse para destruir a la humanidad y, si no se la usa inteligentemente, llegará muy lejos en esa dirección”.

No debemos olvidar que también se elaboran nuevas normas sobre la maquinaria que utiliza IA, de forma que se genere una mayor confianza a los usuarios en la adopción y utilización de nuevos productos.

Las nuevas normas se deben aplicar de la misma manera en todos los Estados miembros, de manera que se establezcan reglas armonizadas para la introducción en el mercado, la puesta en servicio y el uso de los sistemas de IA.

A este respecto, es importante destacar que la propuesta de Reglamento propone un ámbito de aplicación subjetivo y territorial amplio, de forma que incluye a todos los actores en la cadena de valor de IA (proveedores, importadores y distribuidores), también si están empleados en un tercer país, siempre y cuando tengan efectos en la UE, lo que no es ya extraño en la legislación europea⁴¹.

Como hemos adelantado en el epígrafe inmediatamente anterior, la propuesta de Reglamento divide los sistemas de IA en cuatro niveles de riesgo, estableciendo distintas obligaciones en función de su riesgo específico.

58

2.1. SISTEMAS DE IA PROHIBIDOS: se trata de una lista tasada, y de revisión periódica, cuyo uso estaría prohibido al conllevar un riesgo inadmisibles para la seguridad, los derechos fundamentales y la vida.

Se trata de sistemas capaces de manipular el compartimiento humano, predecir información sobre colectivos para identificar circunstancias especiales, sistemas que permitan la puntuación social por parte de los gobiernos o aquellos que impliquen identificación biométrica o videovigilancia masiva en directo por las autoridades en espacios públicos. Estos últimos únicamente serán permitidos para el cumplimiento de la ley y siempre previa autorización judicial o administrativa que, en casos de extrema urgencia, se podrá solicitar con posterioridad a su implementación.

Obviamente ha surgido la polémica con la previsión de que las autoridades puedan utilizar estos sistemas de videovigilancia masiva sin autorización, ya que ellos mismos determinar la “extrema urgencia”.

¿Qué ocurre si posteriormente es denegada la autorización judicial o administrativa?
¿Qué consecuencias jurídicas tendrán los hechos obtenidos mediante estos métodos de videovigilancia masiva directa?

Podemos encontrarnos entonces con la invalidez de las medidas tomadas como consecuencia de la utilización de estos sistemas, con la consiguiente inseguridad tanto para las autoridades como para los ciudadanos.



2.2.SISTEMAS DE IA DE ALTO RIESGO: se trata de sistemas que implican el análisis potencial lesivo en la salud y seguridad o derechos fundamentales para las personas, teniendo a su vez en cuenta las finalidades para las que se contempla su uso.

Nuevamente es un listado tasado y sujeto a revisión periódica para adaptarlo a las nuevas tecnologías.

Si bien no están prohibidos, deben estar sujetos a obligaciones reforzadas que garanticen su uso legal, ético, robusto y seguro.

Estos sistemas abarcan las siguientes áreas:

- Infraestructuras críticas como, por ejemplo, los transportes, que pueden poner en peligro la salud y la vida de los ciudadanos.
- Formación, tanto educativa como profesional, en tanto pueden determinar la carrera de una persona o su acceso a la educación.
- Componentes de seguridad de los productos.
- Empleo y gestión de los trabajadores como, por ejemplo, programas de clasificación de CV.
- Servicios públicos y privados esenciales como, por ejemplo, la gestión crediticia.
- Gestión de migración y asilo o control de fronteras, en la comprobación de documentos.
- Aplicación de leyes, cuando puedan interferir con los derechos fundamentales de las personas como, por ejemplo, la evaluación de la fiabilidad de las pruebas.
- Administración de justicia y procesos democráticos.

59

Estos sistemas necesitan cumplir determinados requisitos para poder ser utilizados. Así, por ejemplo, deben ser sometidos a una evaluación de conformidad y gestión del riesgo durante toda su vida útil, estando cada operador de la cadena de valor sometido a obligaciones específicas, a saber:

- Gobernanza de datos: los datos deben cumplir estándares de calidad y se deben examinar y supervisar posibles sesgos.
- Seguridad y supervisión humana: en última instancia debe haber una persona con capacidad de control para mitigar eventuales riesgos.
- Deber de transparencia: descripción de las características del funcionamiento del sistema e identidad y datos del proveedor.
- Inscripción en una base de datos europea con carácter previo a su puesta a disposición en el mercado.
- Superación del test de conformidad y certificación en función de las especificaciones técnicas requeridas.

Nuevamente debemos realizar consideraciones críticas en esta clasificación.

Claramente, los sistemas relacionados con la salud deberían ser considerados sistemas de alto riesgos.

Sin embargo, como veremos más adelante, sistemas como, por ejemplo, los filtros de correo spam son considerados sistemas de riesgo limitado.

¿Qué ocurre, en consecuencia, si perdemos una cita médica porque un sistema de filtro de correo spam ha desechado un correo y retrasamos la consulta un tiempo que habría sido decisivo para diagnosticar una enfermedad?

¿Debería, entonces, otorgarse esta calificación de riesgo alto, con las obligaciones que conlleva, a todos los sistemas relacionados con un determinado ámbito independientemente de la finalidad para la que estén concebidos? ¿Cómo se debería hacer esta diferenciación?

Es decir ¿cómo se podría delimitar este sistema de filtrado de correo cuando su uso vaya a poder tener consecuencias en el ámbito de salud?

60

Ciertamente, parece que van a existir ciertos sistemas que por su finalidad principal van a ser considerados de riesgo mínimo o nulo, por mucho que sus “decisiones” puedan tener incidencia en ámbitos tan delicados como, por ejemplo, la salud, como acabamos de ver.

2.3.SISTEMAS DE IA DE RIESGO LIMITADO: se trata de sistemas que no suponen un alto riesgo para los derechos y libertades de las personas. Incluyen tecnologías que interactúan con las personas como, por ejemplo, los chatbots o robots conversacionales.

A los proveedores de estos sistemas se les exige el cumplimiento de obligaciones de transparencia, con el fin de hacer a los usuarios conscientes de que están interactuando con una máquina para tomar sus decisiones de manera informada.

Desde nuestro punto de vista, el riesgo más claro está relacionado con los usuarios de esos sistemas. Estamos hablando, por ejemplo, del caso de los menores de edad que, aún habiendo sido informados de estar interactuando con una máquina, no tienen capacidad para discernir las consecuencias de la información que dicho chatbot le esté proporcionando.

¿Deberían, en consecuencia, todas las empresas que utilizan estos sistemas, estén o no sus servicios destinados a menores, contar con sistemas para acreditar la edad del interlocutor? ¿Al menos aquellas en las que sí sea altamente probable que sus usuarios sean menores? ¿Deberían restringir el tipo de información proporcionada a través de esos sistemas para mitigar estos riesgos?



2.4.SISTEMAS DE IA DE RIESGO MÍNIMO O NULO: el resto de sistemas están permitidos y la propuesta de Reglamento no establece obligaciones específicas, ya que representan un riesgo mínimo o nulo para los derechos o la seguridad de los ciudadanos.

Debemos decir que, a día de hoy, la inmensa mayoría de los sistemas de IA entran en esta categoría. Nos estamos refiriendo a aplicaciones tales como videojuegos basados en IA o filtros de correo spam.

Ya hemos analizado las dudas que nos surgen en la clasificación como sistemas de riesgo mínimo o nulo en determinadas utilidades, por ejemplo, de los filtros de correo spam.

En el caso de los videojuegos, las reflexiones están más bien relacionadas con cuestiones de carácter ético, como consecuencia, por ejemplo, de la violencia de su contenido o de las implicaciones en materia de adicción o cambio de conducta por parte de sus usuarios.

En estos casos en que el sistema de IA es considerado de riesgo mínimo o nulo, los agentes de la cadena pueden adherirse a sistemas voluntario de cumplimiento, lo que sin duda reforzará la confianza de los usuarios de estos sistemas.

61

En supuestos de incumplimiento, serán los Estados miembros quienes establecen las normas sobre sanciones, incluidas las multas administrativas aplicables a las infracciones del Reglamento.

La propuesta de Reglamento debe ser revisada y debatida en el Parlamento Europeo y el Consejo, pudiendo por tanto ser objeto de enmiendas. Una vez aprobado, el Reglamento será de aplicación directa en todos los países de la UE, lo que permitirá la deseada regulación y aplicación homogénea.

La Comisión propone la creación de un Comité Europeo de IA que facilitará la IA e impulsará su regulación, si bien las autoridades nacionales de vigilancia deben controlar las nuevas normas.

7. CONCLUSIONES

La IA es una tecnología estratégica y, en este sentido, ofrece ventajas tanto a los ciudadanos, como a las empresas y a, por lo tanto, a la sociedad en su conjunto. Puede aportar mejoras en la eficiencia y la productividad y reforzar la competitividad de la industria europea, a la vez que conlleva una mejora el bienestar de los ciudadanos.

Sin embargo, la visión de la UE es que solo se puede conseguir si el desarrollo de la IA se basa en el respeto de los derechos y valores fundamentales.

En este sentido, la estrategia de la UE es clara: la IA debe ser antropocéntrica, ética y sostenible.

Además, hay dos requisitos que necesariamente deben cumplirse para que el desarrollo de la IA sea un éxito en la UE: medidas que permitan a la UE convertirse en un centro de datos mundial e inversión en tecnologías e infraestructuras, así como en competencias digitales como la alfabetización en datos.

Ambos elementos son clave para reforzar la soberanía tecnológica de Europa basada en los valores y normas europeas.

Es decir, la IA debe estar al servicio de las personas y ser una fuerza positiva para la sociedad.

En este sentido, el Libro Blanco sobre IA propone un enfoque orientado a la regulación y a la inversión, con el objetivo de promover la adopción de IA y abordar los riesgos asociados a determinados usos de esta tecnología.

El Libro Blanco se basa en los principios de “ecosistema de excelencia”, destinado a aportar incentivos adecuados para acelerar la adopción de soluciones basadas en IA en toda la cadena de valor, y “ecosistema de confianza”, aplicando las normas existentes en cuanto a protección de consumidores y protección de datos, así como Directivas en materia de seguridad y responsabilidad del producto, específicamente mientras se carezca de un marco normativo común.

Como hemos analizado, la propuesta de Reglamento plantea un acercamiento basado en el riesgo, haciendo responsables a todos los intervinientes en la cadena de valor de los productos y servicios de IA y estableciendo obligaciones, hasta en los casos de IA con nivel de riesgo limitado, de información y transparencia dirigidas a favorecer la confianza de los consumidores, así como códigos de conducta y sistemas de adhesión de cumplimiento voluntarios.

Esta nueva revolución industrial generada por la IA denominada *Industria 4.0* ha dado lugar a la progresiva automatización de la gran mayoría de los procesos productivos. Ello implica en la necesidad de la especialización de los trabajadores, con el fin de garantizar el nivel más elevado posible de competencia profesional, así como la formación de los usuarios para que puedan familiarizarse con los requisitos tecnológicos de la IA.

Obviamente, la especialización tiene desventajas para el trabajador menos cualificado, por lo que es necesario que los Gobiernos inviertan en educación y acometan otras



reformas para mejorar la redistribución en los tipos de capacidades que necesitarán los trabajadores en el futuro.

Es decir, los recursos humanos deben ir unidos a las inversiones económicas para favorecer la adaptación a la *Industria 4.0* por lo que, más allá de pensar si la IA sustituirá o no trabajadores, es esencial que las próximas generaciones quieran acceder a formación adecuada adaptada al nuevo modelo de trabajo.

Más allá de estas reflexiones, debemos tener en cuenta las limitaciones de la IA ¿podrá la IA liderar un equipo de trabajo, tener en cuenta las circunstancias personales de sus trabajadores o sus mejores cualidades y aspiraciones personales y profesionales? ¿Podrá la IA arreglarse en caso de fallo o error?

Debemos ser conscientes de la importancia del factor humano en el mercado laboral en su conjunto y las consecuencias directas e indirectas de la adaptación de la IA.

Si un contrato de trabajo se extingue por la necesidad del empresario de amortizar o suprimir uno o varios puestos de trabajo siempre que existan causas económicas, técnicas, organizativas o de producción ¿cabe subsumirlo bajo este supuesto si posteriormente el puesto de trabajo es ocupado por un robot que realiza la misma tarea? Como hemos indicado, una solución es que la negociación colectiva garantice la intervención de los representantes de los trabajadores con la emisión de los informes en los casos preceptivos.

63

Es cierto que la Resolución aprobada el 16 de febrero de 2017 consideraba que los efectos del desarrollo e implantación de la IA podrían tener efectos en la viabilidad de los sistemas de seguridad social de los Estados miembros que debería examinarse.

De hecho, en su Anexo hace referencia a la necesidad de comunicar la utilización de sistemas de IA por parte de empresas indicando el número de robots inteligentes que utilizan, los ahorros en las cotizaciones a la seguridad social gracias a la utilización de robótica, y una evaluación de la cuantía y proporción de los ingresos de la empresa procedente de la robótica y de la IA.

Todo ello teniendo en cuenta que, si bien el Parlamento Europeo habló de la necesidad de que la Comisión proponga definiciones europeas comunes de sistema ciberfísico, sistema autónomo, robot autónomo inteligente y sus distintas categorías, todavía no contamos con ellas a pesar de ser cuestión esencial, por ejemplo, en el ámbito de la responsabilidad civil por los daños que se originen por la actuación de estos sistemas de IA.

Y ello es así porque uno de los elementos esenciales del sistema de responsabilidad extracontractual es el referente a la imputabilidad, es decir, que haya posibilidad de culpa en el agente que causa el daño.

La culpa exige, al menos, entender la posibilidad de que exista un daño, aunque no sea intencional, para que pueda imputarse a quien lo ha realizado. Y aquí nuevamente entramos en el debate de que el sistema de IA pueda considerarse una persona jurídica.

Como indica el Parlamento Europeo en su Resolución de 16 de febrero de 2017, cuanta más autonomía tengan los robots, más difícil será considerarlos meros instrumentos en manos de otros agentes y, si pueden tomar decisiones autónomas, las normas tradicionales no bastan para generar responsabilidad jurídica por los daños causados por el sistema de IA, ya que no permiten determinar la parte que ha de hacerse cargo de la indemnización ni exigir a la parte que repare el daño causado. Por ello su prioridad es garantizar que, en el desarrollo de la robótica y los sistemas de IA, los seres humanos tengan en todo momento el control sobre las máquinas inteligentes.

64

En este caso podríamos acudir, como hemos visto, a la responsabilidad civil extracontractual en relación a daños causados por hechos ajenos como, por ejemplo, por falta de cuidado en cosas inanimadas como ocurre con los padres o tutores respecto de los hijos menores o personas con capacidad judicialmente modificada por *culpa in eligendo* o *in vigilando*.

Si calificamos a los sistemas de IA como productos u objetos, podemos abordar el problema desde la legislación de la protección del consumidor y de la reparación de daños por productos defectuosos, tal como ha decidido hacer la Comisión.

Tampoco es sencillo el acercamiento desde el punto de vista del Derecho Penal, si bien la doctrina mayoritaria es favorable, con el sistema jurídico actual, a resolver las posibles causas desde la consideración de los sistemas de IA como objetos muebles.

En definitiva, si bien asistimos a la primera regulación jurídica europea en este ámbito tan complejo, lejos de seguir el camino iniciado en la Resolución de 16 de febrero de 2017, abordando la normativa desde la creación de una personalidad jurídica específica para los robots, especialmente para los más complejos de forma que puedan ser considerados personas electrónicas responsables de causar daños; se ha abordado una propuesta de Reglamento con un acercamiento basado en el riesgo que establece requisitos específicos en función del nivel de riesgo del sistema de IA en concreto y que, adicionalmente, ofrece un sistema de cumplimiento voluntario para aquellos sistemas que presenten un riesgo mínimo o nulo.



Obviamente, la propuesta de Reglamento sufrirá modificaciones hasta su aprobación final y será necesario continuar atentos a la evolución legislativa, si bien no es probable que de las posibles soluciones jurídicas que el Parlamento solicitó a la Comisión estudiar como futuro instrumento legislativo, la relativa a creación de una persona electrónica responsable sea abordada de forma inmediata.

BIBLIOGRAFÍA

- ARMENTA DEU, T. (2021): *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio*. Marcial Pons, Madrid.
- AZUAJE PIRELA, M., y FINOL GONZÁLEZ, D. (2020): “Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones”. *Revista La Propiedad Inmaterial*, núm. 30, pg. 111-146.
- BALCELLS, M. (2020): “Luces y sombras del uso de la inteligencia artificial en el sistema de justicia penal” en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (Eds) *Retos jurídicos de la Inteligencia Artificial*, Aranzadi, Cizur Menor (Navarra).
- BARRIO ANDRÉS, M. (2019): *Derecho de los robots* Ed. Wolters Kluwer, Madrid.
- BARONA VILAR, S. (2021): *Algoritmización del derecho y de la justicia. De la Inteligencia Artificial a la Smart Justice*. Tirant lo Blanch, Valencia.
- BARRAT, J. (2014): *Nuestra invención final*. Paidós, México.
- BONET PÉREZ, J. (2018): “Disrupción tecnológica y trabajo, ¿disrupción también en el ámbito de las relaciones laborales?”, *Revista Mientras Tanto.e*, núm. 169, pg. 4.
- BROZEK, B. y JAKUBIEC, M. (2017): “On the legal responsibility of autonomous machine”, *Artif Intell Law*, pg. 303.
- CALO, R. (2015): “Robotics and the Lessons of Cyberlaw”, *California Law Review*, vol. 103, núm. 3, pg. 515.
- CALO, R. (2016): “Robots as legal metaphors”, *Harvard Journal of Law and Technology*, núm.30, pg. 20-237.

- CASTELLANOS CLARAMUNT, J. y MONTERO CARO, M.D. (2020): Perspectiva constitucional de las garantías de aplicación de la Inteligencia Artificial: la ineludible protección de los derechos fundamentales. *Ius et Scentia*, núm. 6 (2), pg. 72-82.
- CERRILLO I MARTÍNEZ, A. (2019): “El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?”, *Revista General de Derecho Administrativo*, núm. 50, pg. 60-65.
- COTUREL, C. (2016): “¿Podrían las máquinas contratar y despedir trabajadores? Inteligencia Artificial, algoritmos y Smart contracts en el derecho del trabajo”, *Revista del Instituto de Estudios Interdisciplinarios en Derecho Social y Relaciones del Trabajo (IDEIDES)*, núm. 122, pg. 28-34.
- CORVALÁN, J.G. (2017): Inteligencia Artificial y Derechos Humanos (Parte II), *Diario Constitucional y Derechos Humanos*, núm. 157, pg. 38-60.
- DE LA QUADRA-SALCEDO, T. y PIÑAR, J.L., *Sociedad digital y Derecho*, BOE-Red.es, Madrid.
- DENNETT, D.C., (1995): *Consciousness Explained*, Black Bay/Little, Brown ed., Boston.
- DOMÍNGUEZ PECO, E. (2019): “Los robots en el Derecho Penal” en Barrio Andrés, M. *Derecho de los Robots*, Ed. Wolters Kluwer, Madrid.
- FERNÁNDEZ PÉREZ, N. (2021): “La inteligencia artificial como motor de progreso: el difícil equilibrio entre los derechos de propiedad intelectual y la privacidad”, *La Ley Mercantil*, núm. 85, pg. 78.
- GARCÍA MEXÍA, P. (2016): “¿Puede un robot tener responsabilidad civil o penal?” Noticias Jurídicas [Consulta: 13-12-2021].
- GARCÍA SÁNCHEZ, M.D. (2020): “Inteligencia artificial y oportunidades de creación de una personalidad electrónica”, *Ius et Scientia*, vol. 6, núm. 2, pg. 57-63.
- GARCÍA SAN JOSÉ, D. (2021): “Implicaciones jurídicas y bioéticas de la Inteligencia Artificial (IA). Especial consideración al marco normativo internacional” *Cuadernos de Derecho Transnacional*, núm. 13(1), pg. 255-276.
- GUIHOT, M., MATTHEW, F.; SUZOR, N. P. Nudging robots (2017): Innovative solutions to regulate artificial intelligence, *Vand. J. Ent. & Tech. L.*, núm. 20, pg. 385.



- GÓMEZ-RIESCO TABERNERO DE PAZ, J. (2019): Los robots y la responsabilidad civil extracontractual en Barrio Andrés, M. *Derecho de los Robots*, Ed. Wolters Kluwer, Madrid.
- GONZÁLEZ GRANADO, J. (2016): “Derecho y Robots en la Unión Europea: hacia una personalidad electrónica”, Taller de Derechos en <https://tallerdederechos.com/derecho-y-robots-en-la-union-europea-hacia-una-persona-electronica> [Consulta: 13-12-2021].
- HINTZE, A (2016): “Understanding the four types of AI, from reactive robots to self-aware beings”, The Conversation, Understanding the four types of AI, from reactive robots to self-aware beings [Consulta: 19-12-2021].
- LACRUZ MANTECÓN, M.L. (2019): “Cibernética y Derecho Europeo: ¿una inteligencia robótica?” *Diario La Ley*, núm. 9376, Sección Doctrina, 13 de marzo de 2019, Editorial Wolters Kluwer, Madrid.
- MARTÍNEZ DE PISÓN, J. (2017): “Yo, Robot: de la biología a la singularidad. ¿Nuevas preguntas para la Filosofía del Derecho?”, *REDUR*, 15 diciembre 2017, págs. 57-73.
- MARTÍNEZ MARTÍNEZ, R. (2019): “Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo”. *Revista Catalana de Dret Públic*, núm. 58, pg. 64-81.
- NAVAS NAVARRO, S. (2017) “Derecho e inteligencia artificial desde el diseño. Aproximaciones”, *Inteligencia artificial. Tecnología. Derecho*, VV.AA., Tirant lo Blanch, 2017.
- NEVEJANS, N. (2016): Study for Jury Committee European Civil Law Rules In Robotics, Policy Department C Citizens’ Rights and Constitutional Affairs, European Parliament, Brussels, 2016, pg.16.
- NIEVA FENOLL, J. (2018): *Inteligencia artificial y proceso judicial*. Marcial Pons, Madrid.
- PALMERINI, E. (2017): “Robótica y Derecho: sugerencias, confluencias, evolución en el marco de una investigación europea”, *Revista de Derecho Privado*, núm. 32, pg. 97-103.
- PUENTE PÉREZ, E. (2019). “Los robots en el Derecho del Trabajo” en Barrio Andrés, M. *Derecho de los Robots*, Ed. Wolters Kluwer, Madrid.

QUINTERO OLIVARES, G. (2017): “La robótica ante el Derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas”, *Revista Electrónica de Estudios Penales y de la Seguridad*, núm. 7, pg. 9.

SAN MIGUEL CASO, C. (2021): “La aplicación de la Inteligencia Artificial en el proceso ¿un nuevo reto para las garantías procesales?”, *Ius et Scientia*, vol. 77, núm.1, pg. 286-303.

RODOTÁ, S. (2014): *El derecho a tener derechos*. Editorial Trotta, Madrid.

SANTOS GONZÁLEZ, M.J. (2017): “Regulación legal de la robótica y de la inteligencia artificial: retos de futuro”, *Revista jurídica de la Universidad de León*, núm. 4, pg. 39-43.

SEGURA ALASTRUÉ, M. (2019). “Los robots en el Derecho Financiero y Tributario” en Barrio Andrés, M. *Derecho de los Robots*, Ed. Wolters Kluwer, Madrid.

68

SERRANO PÉREZ, M y FERNÁNDEZ ALLER, C. (2021): *Derecho Constitucional e Inteligencia Artificial en La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0. Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes*. Editorial Dykinson, Madrid.

SMITH, B.C. (2019) *The promise of artificial intelligence. Reckoning and judgement*. The MIT Press, Cambridge (Massachusetts).

SOMOLINOS SÁNCHEZ, J.A., (2002): *Avances en la robótica y visión por computador*, Ed. Universidad Castilla-La Mancha, Cuenca.

UNIÓN EUROPEA (2019) *Directrices éticas para una Inteligencia artificial fiable, redactado por el Grupo de expertos de alto nivel sobre inteligencia artificial (IA)*. ISBN 78-92-76-11994-4.

WIENER, N. (1969), *Cibernética y sociedad*, Editorial Sudamericana, Buenos Aires.



REFERENCIAS

¹ <http://www.robotlaw.eu/>

² Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

³ Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza EUROPEA, COM(2020) 65 final.

⁴ Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión COM(2021) 206 final.

⁵ Proyecto de Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

⁶ Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

⁷ Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Inteligencia artificial para Europa COM (2018) 237 final, modificada por el grupo de expertos de alto nivel.

⁸ Recomendación sobre la Ética de la Inteligencia Artificial accesible [en línea] en https://unesdoc.unesco.org/ark:/48223/pf0000379920_spa.page=15.

⁹ Dictamen del Comité Económico y Social Europeo sobre la «Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad» (2017/C 288/01).

⁹ https://ec.europa.eu/info/strategy/international-strategies/sustainable-development-goals_es

¹⁰ Instituto Autor. [China: Un tribunal reconoce derechos a un artículo escrito por un algoritmo de Inteligencia Artificial desarrollado por una empresa \(institutoautor.org\)](https://www.institutoautor.org/) [Consulta: 21-12-2021].

¹¹ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

¹² Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

¹³ Anteproyecto de Ley de Enjuiciamiento Criminal, [210126 ANTEPROYECTO LECRIM 2020 INFORMACION PUBLICA \(1\).pdf \(mjusticia.gob.es\)](https://www.mjusticia.gob.es/web/guest/anteproyecto-de-ley-de-enjuiciamiento-criminal) [Consulta: 13-12-2021].

¹⁴ OECD's annual report on jobs and employment in OECD countries. https://www.oecd-ilibrary.org/employment/oecd-employment-outlook-2019_9ee00155-en. [Consulta: 21-12-2021]

¹⁵ [El futuro del trabajo: Conferencia de alto nivel para debatir la manera en que la UE puede afrontar los retos y aprovechar las oportunidades \(europa.eu\)](https://www.europa.eu). [Consulta: 24-12-2021]

- ¹⁶ <https://www.poderjudicial.es/search/AN/openDocument/1af75e3bf3e5c069/20191125> [Consulta: 21-11-2021].
- ¹⁷ Comisión Mundial sobre el Futuro del Trabajo, Trabajar para un futuro más prometedor, Oficina Internacional del Trabajo, Ginebra, OIT, 2019, p. 10.
- ¹⁸ [BOE.es - BOE-A-2019-2364 Ley 1/2019, de 20 de febrero, de Secretos Empresariales](https://www.boe.es/BOE-A-2019-2364-Ley-1/2019-de-20-de-febrero-de-Secretos-Empresariales). [Consulta: 07-12-2021].
- ¹⁹ Simposio de la OMPI sobre Secretos Comerciales e Innovación. Disponible [en línea] en [E \(wipo.int\)](https://www.wipo.int) [Consulta: 27-10-2021].
- ²⁰ 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)) (2021/C 404/05).
- ²¹ Resolución sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)).
- ²² <https://campusialab.com.ar/wp-content/uploads/2020/07/Carta-e%CC%81tica-europea-sobre-el-uso-de-la-IA-en-los-sistemas-judiciales-.pdf>. [Consulta: 02-12-2021]
- ²³ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Generar confianza en la inteligencia artificial centrada en el ser humano. COM/2019/168 final.
- ²⁴ Estrategia europea de datos. Hacer de la UE un modelo de sociedad capacitada por los datos. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es [Consulta: 02-12-2021]
- ²⁵ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es#ejemplos-de-utilizacin-de-datos-industriales-y-comerciales [Consulta: 02-12-2021].
- ²⁶ <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review> [Consulta: 02-12-2021].
- ²⁷ https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_es [Consulta: 05-12-2021].
- ²⁸ <https://www.horizonteeuropa.es/> [Consulta: 12-10-2021].
- ²⁹ https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/recovery-and-resilience-facility_es [Consulta: 11-12-2021].
- ³⁰ <https://www.idc.com/getdoc.jsp?containerId=US45599219> [Consulta: 21-10-2021].
- ³¹ <https://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017> [Consulta: 12-10-2021].
- ³² La invención de la ingeniería neuromórfica se atribuye a Carver Mead, un ingeniero eléctrico estadounidense formado en Caltech que a finales de los años 60 inició el estudio del diseño de circuitos integrados y algoritmos capaces de imitar el comportamiento del sistema nervioso de los animales.
- ³³ Inteligencia Artificial para Europa [COM (2018)237].



¿Estamos caminando hacia el reconocimiento de la personalidad jurídica a los robots en la Unión Europea?

³⁴ Plan coordinado sobre la inteligencia artificial [COM (2018)795].

³⁵ <https://www.ai4eu.eu/> [Consulta: 12-11-2021].

³⁶ https://europa.eu/investeu/home_es [Consulta: 12-11-2021].

³⁷ Fáciles de encontrar, accesibles, interoperables y reutilizables, tal como establece el informe final y el Plan de Acción del Grupo de Expertos en datos FAIR de la Comisión, de 2018 Turning FAIR into reality (europa.eu).

³⁸ OECD Principles on Artificial Intelligence - Organisation for Economic Co-operation and Development.

³⁹ Directrices éticas para una IA fiable - Publications Office of the EU (europa.eu).

⁴⁰ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Generar confianza en la inteligencia artificial centrada en el ser humano COM (2019) 168.

⁴¹ Véase, a este respecto, el Reglamento General de Protección de Datos (REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

