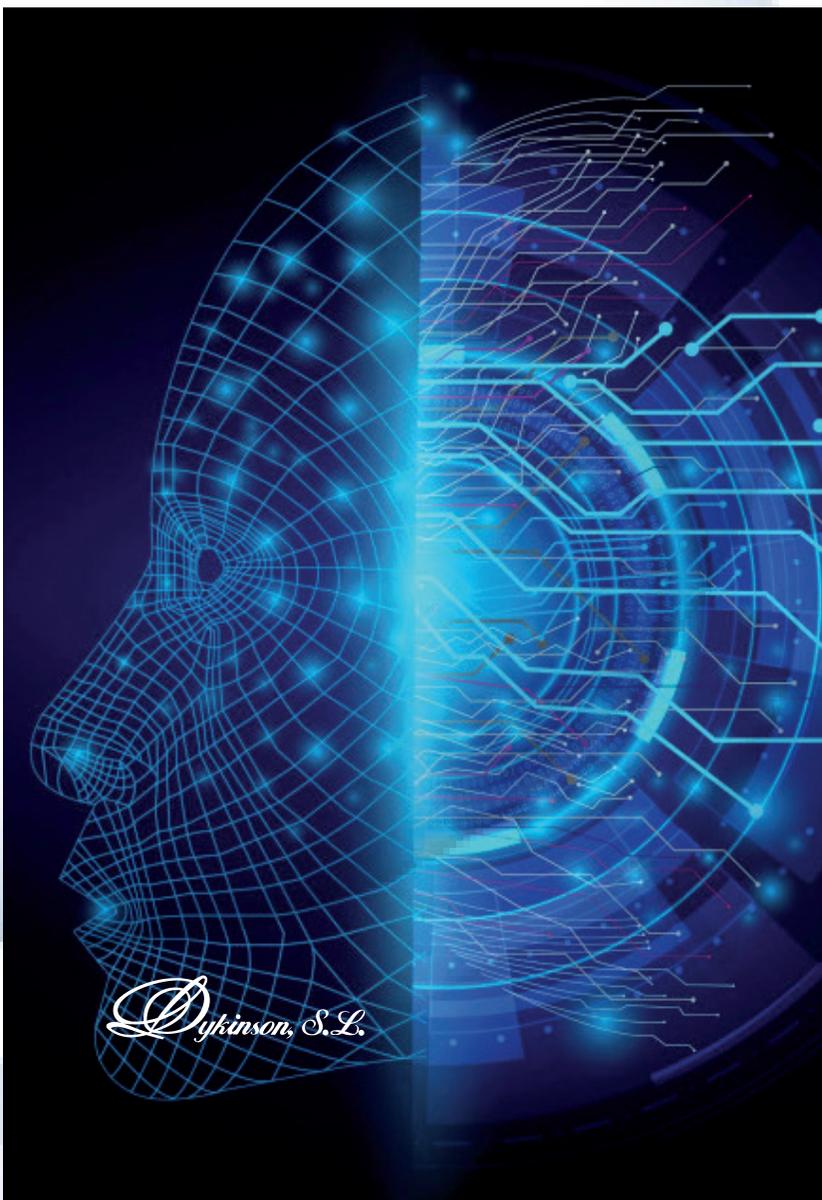


**ASPECTOS LEGALES  
DE LA INTELIGENCIA ARTIFICIAL**  
**Personalidad Jurídica de los Robots,  
Protección de Datos y Responsabilidad Civil**

**RAMÓN HERRERA DE LAS HERAS**



*Dykinson, S.L.*



**Colección  
IA, Robots, y Bioderecho**



# **ASPECTOS LEGALES DE LA INTELIGENCIA ARTIFICIAL**

**Personalidad Jurídica de los Robots,  
Protección de Datos y Responsabilidad Civil**

## **Colección IA, ROBOTS, Y BIODERECHO**

### **Directores**

FRANCISCO LLEDÓ YAGÜE  
Catedrático de Derecho Civil de la Universidad de Deusto

IGNACIO BENÍTEZ ORTÚZAR  
Catedrático de Derecho Penal de la Universidad de Jaén

CRISTINA GIL MEMBRADO  
Profesora Titular de Derecho Civil de la Universidad de las Islas Baleares

ÓSCAR MONJE BALMASEDA  
Profesor Titular de Derecho Civil de la Universidad de Deusto

### **Coordinadores**

M<sup>a</sup> JOSÉ CRUZ BLANCA  
*Profesor titular de Derecho Penal de la Universidad de Jaén*

IGNACIO LLEDÓ BENITO  
*Profesor Derecho Penal de la Universidad de Sevilla. Profesor titular acreditado (ANECA)*

### **Comité científico**

LORENZO MORILLAS CUEVA  
*Catedrático de Derecho Penal de la Universidad de Granada*

MANUEL MARCHENA GARCÍA  
*Presidente de la Sala Segunda del Tribunal Supremo*

PILAR FERRER VANRELL  
*Catedrática de Derecho Civil de la Universidad de las Islas Baleares*

JOSÉ ÁNGEL MARTÍNEZ SANCHIZ  
*Notario. Académico de "número" de la Real Academia de Legislación y Jurisprudencia*

VICTORIO MAGARIÑOS BLANCO  
*Notario y miembro de la Comisión General de Codificación*

PIERRE LLUIGI D'ELLOSSO  
*Fiscal General de la República Emérito. Fiscal Nacional Antimafia (Italia)*

ALICIA SÁNCHEZ SÁNCHEZ  
*Magistrado-Juez Registro Civil de Bilbao*

LUCÍA RUGGERI  
*Professore ordinario di Diritto privato presso Università degli Studi di Camerino*

CARMEN OCHOA MARIETA  
*Directora médico ura, Cer.Santander,S.L, Medicina de la reproducción*

MARIAN M. DE PANCORBO  
*Catedrática de Biología Celular, Coordinadora Centro de Investigación Lascaray Ikergunea / Lascaray Research Center, Investigadora Principal Grupo biomics / biomics Research Group*

LUIS MARTÍNEZ LÓPEZ  
*Catedrático de Lenguajes y Sistemas Informáticos de la Universidad de Jaén*

HUMBERTO NICANOR BUSTINCE SOLA  
*Catedrático de Ciencias de la Computación e Inteligencia Artificial de la Universidad Pública de Navarra*

# **ASPECTOS LEGALES DE LA INTELIGENCIA ARTIFICIAL**

## **Personalidad Jurídica de los Robots, Protección de Datos y Responsabilidad Civil**

---

**RAMÓN HERRERA DE LAS HERAS**

*Profesor Titular de Derecho Civil de la Universidad de Almería*

 *Dykinson, S.L.*

No está permitida la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (art. 270 y siguientes del Código Penal).

Diríjase a Cedro (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra. Puede contactar con Cedro a través de la web [www.conlicencia.com](http://www.conlicencia.com) o por teléfono en el 917021970/932720407

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial  
Para mayor información, véase [www.dykinson.com/quienes\\_somos](http://www.dykinson.com/quienes_somos)

© Copyright by  
Ramón Herrera de las Heras  
Madrid

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid  
Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69  
e-mail: [info@dykinson.com](mailto:info@dykinson.com)  
<http://www.dykinson.es>  
<http://www.dykinson.com>

ISBN: 978-84-1122-109-2  
Depósito Legal: M-3712-2022

ISBN electrónico: 978-84-1122-162-7

Preimpresión por:  
*Besing Servicios Gráficos S.L.*  
e-mail: [besingsg@gmail.com](mailto:besingsg@gmail.com)

# ÍNDICE

PRÓLOGO .....	9
<b>CAPÍTULO I. INTRODUCCIÓN A LA INTELIGENCIA ARTIFICIAL DESDE UNA PERSPECTIVA LEGAL.....</b>	<b>11</b>
1. La importancia de la inteligencia artificial en nuestros días .....	11
2. Aplicaciones de la inteligencia artificial.....	14
3. Concepto de inteligencia artificial.....	18
4. La inteligencia artificial y el Derecho. Los retos ante la necesaria adaptación legislativa .....	21
<b>CAPÍTULO II. INTELIGENCIA ARTIFICIAL, ROBOTS Y PERSONALIDAD JURÍDICA .....</b>	<b>29</b>
1. Concepto de robot.....	29
2. La personalidad jurídica.....	32
3. La Personalidad de los robots .....	34
3.1. ¿Hacia una personalidad electrónica? .....	36
3.2. El Robot como cosa .....	39
3.2.1. <i>Imposibilidad de los robots para ser titulares de derechos y obligaciones.....</i>	<i>40</i>
3.2.2. <i>La personalidad de los robots como medio para hacer frente a la responsabilidad civil.....</i>	<i>44</i>
3.2.3. <i>Un nuevo estatus como cosa .....</i>	<i>47</i>

<b>CAPÍTULO III. LA INTELIGENCIA ARTIFICIAL Y LA NECESARIA PROTECCIÓN DE LA PRIVACIDAD .....</b>	<b>51</b>
1. Concepto del Derecho a la protección de datos .....	51
2. Privacidad, protección de datos e inteligencia artificial.....	58
3. Inteligencia Artificial y protección de datos en tiempos de pandemia .....	67
<b>CAPÍTULO IV. INTELIGENCIA ARTIFICIAL, ROBOTS Y RESPONSABILIDAD CIVIL .....</b>	<b>75</b>
1. La responsabilidad civil en el ámbito de la Inteligencia Artificial .....	75
2. ¿Pueden los robots ser civilmente responsables de los daños ocasionados por ellos? .....	79
3. Sistema de responsabilidad civil por los daños producidos como consecuencia de sistemas de inteligencia artificial .....	84
3.1. El régimen de responsabilidad civil aplicable actualmente: La Directiva 85/374 y los daños provocados por la inteligencia artificial. ....	86
3.2. El régimen de responsabilidad civil en la futura legislación europea sobre inteligencia artificial .....	89
3.2.1. <i>El productor</i> .....	91
3.2.2. <i>La responsabilidad civil del desarrollador del software</i> .....	94
3.2.3. <i>Responsabilidad civil del operador</i> .....	98
3.3. La necesaria actualización de conceptos recogidos en la Directiva 85/374 .....	106
3.4. La relación de causalidad .....	108
3.5. Seguro, límite de la cuantía y plazo de prescripción .....	110
<b>BIBLIOGRAFÍA .....</b>	<b>115</b>

## PRÓLOGO

La presente monografía nace con la intención de llevar a cabo un estudio amplio sobre distintos aspectos legales relacionados con la inteligencia artificial. El libro está dividido en cuatro capítulos en los que se trata, además de una introducción, la personalidad de los robots dotados con inteligencia artificial, la privacidad y protección de datos en el uso de esta técnica y la responsabilidad civil de los daños producidos como consecuencia de la aplicación de técnicas de inteligencia artificial.

El primero de los capítulos, a modo de introducción, plantea, por un lado, las distintas aplicaciones para las que la inteligencia artificial puede ser hoy día útil, así como un concepto de esta que nos permita abordar con claridad los aspectos legales que pudieran verse afectados. Finaliza este capítulo con un estudio sobre la relación que la inteligencia artificial tiene con el mundo del Derecho, especialmente en el campo del Derecho privado que, como se podrá comprobar, es muy amplia y variada y plantea un elevado número de desafíos a los que el legislador deberá dar respuesta.

El segundo capítulo se dedica a un aspecto que genera un amplio debate entre la doctrina, como es el de la posibilidad de otorgar personalidad a los robots dotados con inteligencia artificial. Para ello, primero se delimita el concepto del robot y se lleva a cabo un estudio doctrinal sobre las distintas posturas existentes sobre la materia. De este modo, como se podrá comprobar más adelante, se plantean distintas opciones que van desde la creación de una personalidad específica para los robots a la negación de esta y su necesaria configuración como cosa. Todo ello tendrá una indudable relevancia pues, dependiendo de la respuesta final, se abrirá, o no, la posibilidad de que los robots puedan ser sujetos de derechos y obligaciones y, como tales, venir obligados al pago de impuestos o a asumir las indemnizaciones de producirse daños durante su uso o actividad.

El tercero de los capítulos versa sobre un tema de máxima actualidad, que no es otro que la problemática que la inteligencia artificial puede generar en torno a la privacidad de las personas. Así, comenzando por el estudio de esa privacidad, se avanza hacia el concepto de protección de datos en la nueva legislación europea y nacional, para finalizar con el análisis de los

riesgos que esta técnica puede conllevar si su uso es desmedido o desproporcionado. Se estudiarán los principios básicos que harán compatible el uso de estas herramientas con la protección de la privacidad.

El último de los capítulos aborda el tema de la responsabilidad civil por los daños producidos en el uso de técnicas de inteligencia artificial, así como la posibilidad de establecer seguros en este ámbito. Finaliza el capítulo con el estudio sobre la cuantía de las indemnizaciones y los plazos de prescripción.

# CAPÍTULO I.

## INTRODUCCIÓN A LA INTELIGENCIA ARTIFICIAL DESDE UNA PERSPECTIVA LEGAL

### 1. LA IMPORTANCIA DE LA INTELIGENCIA ARTIFICIAL EN NUESTROS DÍAS

La importancia de la inteligencia artificial en el mundo actual está fuera de toda duda. Una importancia que irá a más en los próximos años y ante la que, como sucede con cualquier otra tecnología novedosa en la sociedad, el mundo del Derecho ha de permanecer vigilante para poder adecuar las normas actuales a las nuevas circunstancias y necesidades. Y ello para, por un lado, dar seguridad a los ciudadanos como consumidores de las aplicaciones con inteligencia artificial y, por otro, para configurar un entorno jurídico seguro que permita un desarrollo económico y científico que haga que nuestra sociedad siga avanzando. Ambos elementos son, en una sociedad avanzada, no solo compatibles, sino indisolubles.

Para hacernos una idea de la magnitud del impacto de esta ciencia en el futuro de la economía mundial, basta con pensar que la Unión Europea estima que la inversión público privada en inteligencia artificial hasta el año 2027 alcanzará unos 160.000 millones de euros, situándose como una piedra angular de su política de investigación en la próxima década<sup>1</sup>. El uso de la inteligencia artificial en las empresas internacionales ha aumentado un 25% en el año 2019 y las 15 grandes empresas mundiales han invertido más de 20.000 millones de dólares, destinando más de 15.000 millones de dólares a la creación de startups en este ámbito<sup>2</sup>.

El reciente informe de 2019 realizado por la Universidad de Stanford, *Artificial Intelligence Index Report*, daba muestras de lo trascendental de la in-

---

1 Comisión Europea (2018), *Coordinated Plan on the development and use of Artificial Intelligence Made in Europe*, pág. 2

2 Vid. PEDREÑO MUÑOZ, A. y MORENO IZQUIERDO, L.: “El impacto económico de la Inteligencia Artificial”, *Big Data e Inteligencia Artificial. Una visión económica y legal de estas herramientas disruptivas*, Ed. Universidad de Valencia, 2018, pág. 9

teligencia artificial en distintos aspectos económicos de Estados Unidos. Así, las ofertas de empleo relacionadas con la inteligencia artificial han pasado de ser el 0,26% en 2010 a convertirse en el 1,32% en 2019. En ese mismo periodo, la inversión en nuevas empresas del sector se ha multiplicado al pasar de escasamente 1.300 millones de dólares a más de 40.000 millones<sup>3</sup>. Magnitudes tales que hacen prever que el crecimiento seguirá siendo sostenido durante muchos años.

Algunos estudios señalan que el impacto en el PIB mundial de la inteligencia artificial será de un 14%.<sup>4</sup> Otros llegan a detallar que, en países como Estados Unidos, el crecimiento del valor añadido generado por la inteligencia artificial pasará del 2,6% al 4,6% en 2035. En estas magnitudes, para España podría significar el aumentar entre un 1,7% y un 2,5% del PIB en las próximas dos décadas<sup>5</sup>. Tal es la importancia que está tomando esta tecnología que el Gobierno de España aprobó recientemente una Estrategia Nacional de Inteligencia Artificial con la que pretende hacer frente a los retos que deberemos afrontar los próximos años<sup>6</sup>.

También la inteligencia artificial removerá los cimientos del mundo laboral tal y como lo conocemos hoy. Por un lado, abrirá nuevas expectativas laborales a miles de empleados cualificados y, por otro, pondrá en riesgo muchos de los empleos tradicionales, aun hoy existentes. Algunos estudios señalan la posibilidad de que en los próximos años el 14% de los puestos de trabajo que actualmente ocupamos los humanos podrían ser reemplazados por los robots<sup>7</sup>. Un reciente estudio del *BBVA Research* advierte que, si bien el avance de la inteligencia artificial y la robótica generarán en nuestro país nuevos puestos de trabajo, también se automatizarán muchas tareas que podrían poner en riesgo hasta un 36% de los puestos de trabajo actuales<sup>8</sup>. Tanto es así que los expertos se plantean algunas medidas, como la de la cotización a la seguridad social de los robots, sobre lo que posteriormente hablaremos, que hasta hace pocos años parecerían ciencia ficción.<sup>9</sup> Es evidente que igualmente tendrá efectos en la productividad

---

3 STANFORD (2019) *The AI Index 2019 Annual Report*, AI Index Steering Committee, Human-Centered AI Institute, Stanford University. Accesible en [https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai\\_index\\_2019\\_report.pdf](https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf)

4 PWC (2017) *Exploiting the AI Revolution*, pág. 1. Accesible en <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>, pág. 1

5 ACCENTURE, 2016 *Inteligencia artificial, el futuro del crecimiento*, pág. 16

6 Gobierno de España (2019) *Estrategia Española de I+D+i en Inteligencia Artificial*

7 Profesiones como teleoperadores, empleados de banca, limpieza, logística o atención al cliente son algunas de las que se señalan entre las que los robots pueden sustituir a los humanos. Vid. PUGLIANO, J.: *The Robots are Coming: A Human's Survival Guide to Profiting in the Age of Automation*, Ed. Ulysses Press, 2017, pág. 32

8 BBVA Research (2018), *¿Cuán vulnerable es el empleo en España a la revolución digital?*, pág. 13

9 Señala GÓMEZ SALADO en este sentido que “la enorme complejidad que supone ejecutar y articular, jurídicamente, un nuevo mecanismo en el que tengan cabida las cotizaciones de los robots a

laboral pues, según se recoge en un reciente informe de *ACCENTURE*, esta técnica podría aumentar hasta un 40% la productividad en el trabajo en los próximos años<sup>10</sup>.

Como cualquier revolución científica, los avances en esta materia comportan mejoras, pero también riesgos e incertidumbres que han de ser tenidos en cuenta de cara a evitar mayores problemas. Es lo que ha hecho la Organización Internacional del Trabajo que ya advirtió en el año 2019 que, si bien la inteligencia artificial y la robótica crearían miles de nuevos puestos de trabajo, también generarían grandes retos en el ámbito laboral que tendrán que ser tenidos en cuenta por los legisladores<sup>11</sup>.

Las aplicaciones prácticas de la inteligencia artificial se ven, y se verán aún más en el futuro, tanto en el sector público como en el privado. Por lo que respecta al primero, distintos países utilizan ya la inteligencia artificial para diseñar políticas públicas o para, como en ha sucedido en la reciente crisis del COVID-19, tomar medidas de control de movilidad de la población. Esto, que como más tarde veremos plantea inconvenientes con el respeto a la privacidad y el derecho a la protección de datos, se ha revelado también como una herramienta muy útil a la hora de intentar frenar el virus. Por otro lado, en el sector privado la irrupción de esta ciencia ha sido notable. *IBM* sostiene que la inteligencia artificial será usada en un plazo no superior a dos años por el 90% de las empresas, ya sea para sus procesos de producción, para fidelizar, para buscar clientes o para cualquier otra circunstancia<sup>12</sup>.

Todo ello hace necesario, como señalaba, que el mundo del Derecho, tras un debate sosegado y prolongado en el tiempo, realice las reformas legales oportunas. Es en esa línea en la que están las autoridades europeas que, como posteriormente analizaré, han realizado una propuesta para modificar la actual Directiva 85/374 en materia de responsabilidad civil por los daños causados por los productos defectuosos. En esta monografía trataré de realizar un análisis crítico de las distintas propuestas doctrinales y legislativas existentes en la actualidad, relacionadas con el Derecho civil. Concretamente me centraré en tres cuestiones de máxima actualidad.

---

*la Seguridad Social en favor del progreso social, y sin que ello represente una pérdida de inversiones y, por lo tanto, un menor crecimiento económico.*” Cfr. GÓMEZ SALADO, M.A.: “Robótica, empleo y seguridad social. La cotización de los robots para salvar el estado del bienestar”, en *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Vol. 6, n°3, 2018, pág. 143

10 ACCENTURE, 2016 *Inteligencia artificial, el futuro del crecimiento*, pág. 14

11 Organización Internacional del Trabajo (2019), *Trabajar para un futuro más prometedor*, pág. 10

12 “La inteligencia artificial tendrá un impacto económico de 16 billones de dólares”, en *El Economista*, 7 de enero de 2020. Accesible en <https://www.economista.com.mx/tecnologia/La-inteligencia-artificial-tendra-un-impacto-economico-de-16-billones-de-dolares-en-2030-20200107-0038.html>

La primera de ellas versa sobre la posibilidad de dotar a los robots de algún tipo de personalidad legal, ya sea física o jurídica, y, de ser así, conocer las consecuencias que ello traería consigo. La responsabilidad, la posibilidad de ser titular de derechos y de obligaciones y otras cuestiones de interés. También estudiaré la necesaria compatibilidad entre el uso y desarrollo de la inteligencia artificial con la protección de la privacidad de los ciudadanos. Analizaré los límites establecidos en el Reglamento Europeo de Protección de Datos sobre el uso masivo de los mismos por parte de la inteligencia artificial. Por último, pero quizá uno de los puntos más polémicos, me referiré a la responsabilidad civil derivada de los daños provocados por aplicaciones o robots con inteligencia artificial. De este modo, examinaré las propuestas realizadas tanto por la Comisión Europea como por el Parlamento Europeo para adaptar el sistema de responsabilidad civil actual a los nuevos riesgos generados por la inteligencia artificial, incluyendo la posible exigencia de un seguro de responsabilidad civil obligatorio y el establecimiento de un fondo de compensación para reparar los daños causados.

## 2. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL

Antes de iniciar el estudio en profundidad de los aspectos civiles más destacados en el ámbito de la inteligencia artificial, se hace necesario conocer, al menos someramente, algunas cuestiones básicas relacionadas con esta ciencia. De este modo, saber para qué puede usarse y, de hecho, para qué se usa ya y podrá usarse en el futuro, puede darnos una idea clara de la amplia problemática jurídica que esta técnica puede llegar a generar. Es necesario igualmente tener un concepto básico de lo que realmente es la inteligencia artificial, aunque como posteriormente veremos, se trata de una ciencia amplia que puede tener distintas acepciones, según se detalle más o menos su aplicación.

Quizá el hito que hizo saltar la inteligencia artificial a la fama fue el de la victoria de Deep Blue en 1997, una máquina dotada con inteligencia artificial capaz de aprender en cada partida de ajedrez sobre el campeón mundial de la época, Gary Kasparov. Aquella victoria, aún admirada hoy día, fue un antes y un después en la atención de los ciudadanos. También fue mundialmente conocido el caso del concurso cultural *Jeopardy*, en el que también fue un ordenador ganador en el año 2011. Incluso antes de estos conocidos y llamativos avances, en la década de los ochenta, la inteligencia artificial era ya utilizada en la industria.

BRYSON sostiene que la inteligencia artificial no es que haya evolucionado en lo que puede hacer, sino en “*lo que hacemos con ella*”<sup>13</sup>. Hoy son múltiples las aplicaciones dotadas con inteligencia artificial, unas ya comercia-

---

<sup>13</sup> BRYSON, J.J.: *La última década y el futuro del impacto de la IA en la sociedad*, Open Mind, 2017, pág. 3

lizadas que forman parte de nuestro día a día y otras en fase de pruebas o estudio que pronto llegarán al mercado. Así, muchas empresas cuentan ya con asistentes virtuales con los que se pueden mantener conversaciones y realizar consultas sin que el ser humano participe en las respuestas que se dan.

Las plataformas televisivas de pago te ofrecen unos productos u otros según los datos que van obteniendo de tus visualizaciones. Van aprendiendo de tus preferencias. También usan la inteligencia artificial para asegurarse de que la calidad de la imagen de sus emisiones es la mejor posible en cada momento<sup>14</sup>. Recientemente se ha dado un paso más en los medios audiovisuales tras la creación de un canal de televisión que decide la emisión de sus contenidos en base a la inteligencia artificial<sup>15</sup>. Lo mismo sucede con las plataformas musicales en las que, según tus gustos, te programan listas de reproducción que se acerquen al tipo de música que has escuchado con anterioridad. Estas aplicaciones procesan una gran cantidad de datos que son usados para proponer distintas opciones que pueden coincidir con tus gustos.

El reconocimiento de voz para los asistentes de los teléfonos o altavoces inteligentes se han introducido en nuestras casas con absoluta normalidad. Si la aparición del buscador de *Google* en 1996 supuso una revolución a nivel mundial, podemos hacernos una idea del impacto que tendrá la inteligencia artificial teniendo en cuenta que el 50% de las búsquedas que se realizarán los próximos años serán por voz, utilizando técnicas de inteligencia artificial<sup>16</sup>. Lo mismo sucede con el reconocimiento facial, hoy instalado en casi todos los teléfonos inteligentes y pronto en los aeropuertos para identificación de los pasajeros. Como más tarde veremos, todos estos datos tendrán una especial consideración en lo referente a su protección.

También se usan con asiduidad los llamados *bots*, diminutivo de robot y que lleva aparejada una tarea simple. Son programas que pueden imitar el comportamiento de los humanos y son capaces de realizar algunas tareas de manera automática. Su utilización es muy habitual como herramienta de atención al cliente, en las que normalmente intentan solventar dudas o resolver cuestiones sencillas. También aparecen cada vez más en las redes

---

14 Netflix, por ejemplo, utiliza inteligencia artificial para conocer cuando va a haber picos de mucha demanda simultánea y da una calidad u otra, según el tráfico de datos sea mayor o menor. Vid. “Como usa Netflix la inteligencia artificial”, en *Foundation Robótica*, 15 de agosto de 2019. Accesible en <https://foundationrobotica.com/como-usa-netflix-la-inteligencia-artificial/>

15 “Selekt, el primer canal de televisión cuya parrilla la decide una inteligencia artificial”, en *El País*, 5 de febrero de 2021

16 “Just say it: The future of search is voice and personal digital assistants”, en *Campaign*, 25 de abril de 2016. Accesible en <https://www.campaignlive.co.uk/article/just-say-it-future-search-voice-personal-digital-assistants/1392459>

sociales como instrumentos para multiplicar la difusión de determinadas noticias, en ocasiones falsas, lo que multiplica los riesgos que pueden ocasionar.

Igualmente, en la sanidad, la inteligencia artificial se abre paso con la detección precoz de enfermedades o con los robots quirúrgicos. En el ámbito militar son cada vez más habituales las aplicaciones de inteligencia artificial, así como en el transporte terrestre, con los coches autónomos, o en el aéreo, con los drones capaces de volar solos. Tampoco queda fuera el ámbito económico, puesto que la inteligencia artificial participa en muchas ocasiones en transacciones financieras o ventas online, en ocasiones generando graves consecuencias<sup>17</sup>.

Otra de las aplicaciones que más controversia generan es la de su uso por los operadores jurídicos, llegando incluso a poder ser tenida en cuenta a la hora de tomar decisiones judiciales<sup>18</sup>. CÁCERES define esta posibilidad como una “*disciplina híbrida dedicada al desarrollo de programas cuyos productos finales, de ser atribuibles a un humano, presupondrían el procesamiento inteligente de la información por parte de un operador jurídico*”<sup>19</sup>. Según el informe del Consejo General de la Abogacía Española, la inteligencia artificial es uno de los grandes campos de transformación del sector, cuyo uso y aplicación es cada día más amplio<sup>20</sup>.

Para hacerse una idea de lo trascendental que es en nuestros días la inteligencia artificial, basta pensar en el papel que en la lucha contra la pandemia del coronavirus COVID-19 ha tenido. Muchos países utilizaron aplicaciones dotadas de inteligencia artificial que dieron un resultado muy positivo. Concretamente, Corea del Sur implementó una aplicación con la que monitorizar a todos aquellos que hubiesen estado en de áreas de alto contagio para luego hacer un seguimiento de su estado sin movilizar personal sanitario, localizándolos vía GPS, todo ello para asegurarse que ninguno abandonaba el confinamiento<sup>21</sup>. En España, el Gobierno encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial el desarrollo de diversas

---

17 Tanto es así que en la Bolsa de Nueva York y en el Nasdaq tres cuartas partes de las operaciones bursátiles son hechas por aplicaciones de inteligencia artificial. Vid. “Trading algorítmico: cómo funcionan y qué tienen que ver los algoritmos con la caída de la bolsa de Wall Street”, *BBC*, 6 de febrero de 2018, accesible en <https://www.bbc.com/mundo/noticias-42960565>

18 Muchos son ya los despachos de abogados que cuentan con herramientas con tecnología basada en la inteligencia artificial que les ayuda

19 CÁCERES, E.: “Inteligencia Artificial, Derecho y E-Justice”, en *Boletín Mexicano de Derecho Comparado*, n° 116, 2006, pág. 606

20 Consejo General de la Abogacía Española (2019), *Abogacía futura 2020: Áreas de negocio*

21 Vid. Corea del Sur: contra el coronavirus, tecnología. (2020). *El País*, 14 de marzo. Accesible en <https://elpais.com/tecnologia/2020-03-13/corea-del-sur-contra-el-coronavirus-tecnologia.html>

actuaciones para la gestión de la crisis sanitaria del COVID-19<sup>22</sup>. Con esta aplicación, las autoridades españolas pretendían disponer de información contrastable sobre la movilidad de todos los ciudadanos, antes y durante el confinamiento, con el objetivo de desarrollar un software que pudiese “*recopilar todos los datos y mejorar la eficiencia operativa de los servicios sanitarios, así como mejorar la atención y accesibilidad por parte de los ciudadanos*”<sup>23</sup>. Esta medida ha generado un amplio debate jurídico sobre la compatibilidad del uso masivo de datos para conocer nuestra ubicación con el derecho a la privacidad. Más tarde abordaré la cuestión con detenimiento.

Como acabamos de ver, todos estos avances en materia de inteligencia artificial generan múltiples beneficios y nos facilitan la vida, pero también se abre la puerta a ciertos riesgos a los que el Derecho debe de dar también una respuesta que permita asegurar, por un lado, su desarrollo e implementación y, por otro, la salvaguarda de los derechos de los ciudadanos. Algunos autores han llegado a advertir que, a medida que avanza la inteligencia artificial, los riesgos de que genere algún tipo de daño aumentan exponencialmente y ponen como ejemplo algunos casos en los que estos sistemas han llegado a discriminar a personas por su raza, edad o género y el papel de esta tecnología en la difusión de bulos y de desinformación. Esos posibles daños, apuntan, “*pueden generar una problemática jurídica que vaya desde las demandas judiciales y multas a daños reputacionales y destrucción del valor para los accionistas*”<sup>24</sup>.

Uno de los retos que afrontaremos en los próximos años es el de encontrar el equilibrio necesario entre la protección de los derechos de los ciudadanos y el avance tecnológico de nuestra época. A ese reto, como a lo largo del presente trabajo veremos, debe contribuir la legislación civil, que se convertirá en un elemento esencial para configurar esta técnica.

---

22 Según hizo público el Gobierno, la aplicación con inteligencia artificial que desarrolló tenía el objetivo de “*utilizar los datos globales recogidos a través de estas apps sanitarias, junto al nuevo estudio de movilidad del Instituto Nacional de Estadística (INE), para definir la estrategia de reversión de las medidas de confinamiento.*” Vid. “La app del Gobierno contra el coronavirus ya está disponible: autodiagnóstico y consejos con geolocalización opcional”, *eldiario.es*, 6 de abril de 2020, accesible en [https://www.eldiario.es/tecnologia/Gobierno-coronavirus-disponible-geolocalizacion-opcional\\_0\\_1013849187.html](https://www.eldiario.es/tecnologia/Gobierno-coronavirus-disponible-geolocalizacion-opcional_0_1013849187.html)

23 BOE nº86, de 28 de marzo de 2020

24 Ponen el ejemplo de “*un sistema de inteligencia artificial que decide sobre la marcha dónde colocar los anuncios de empleo en línea podría dirigir injustamente los anuncios de empleos mejor remunerados a los visitantes masculinos de un sitio web porque los datos del mundo real muestran que los hombres suelen ganar más que las mujeres. Del mismo modo, una empresa de servicios financieros que utiliza la IA para examinar las solicitudes de hipotecas podría descubrir que su algoritmo discrimina injustamente a las personas por factores que no son socialmente aceptables, como la raza, el género o la edad.*” Cfr. SAIF, I. y AMMANATH, B.: “Trustworthy AI is a framework to help manage unique risk” en *MIT Technology Review*, 25 de marzo 2020

### 3. CONCEPTO DE INTELIGENCIA ARTIFICIAL

Aunque ya en el S.XVII una familia de relojeros suizos fue capaz de construir unos *androides* que podían escribir, dibujar o tocar el órgano<sup>25</sup>, el origen de esta ciencia se remonta a los años 40, cuando Allan Turing y Grey Walter crearon las primeras máquinas inteligentes que, una década después, hicieron la transición entre el sistema decimal y la lógica binaria<sup>26</sup>. Walter construyó algunos de los primeros robots de la historia y Turing no solo fue famoso por crear la legendaria máquina *Enigma*, sino que inventó el test de Turing, que determinaba cuando se encontraban ante una máquina inteligente. Como explican HOCHÉL y GÓMEZ MILÁN, el test de Turing consiste en el estudio de una conversación que mantenía una persona con el sistema en el que se encontraba instalado el software de inteligencia artificial. Si esa persona era incapaz de determinar cuál de los dos era el ordenador, se consideraba que el sistema tenía una inteligencia comparable a la humana<sup>27</sup>. Esta explicación es interesante porque, como luego veremos, uno de los elementos que caracteriza a esta ciencia es precisamente la cercanía con la inteligencia humana.

No fue sino más de una década después cuando se acuñó el término de inteligencia artificial, concretamente en 1956, año en el que McCarthy, Minsky y Shannon lo definieron en la Conferencia de Dartmouth como el hecho de conseguir que una máquina pudiese razonar como un ser humano, aprender de sí misma y ser capaz de resolver problemas *más o menos complejos*<sup>28</sup>.

A pesar de que el concepto de inteligencia artificial es complejo y que, como señala la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, ninguna de las definiciones ha sido aun aceptada de manera universal<sup>29</sup>, son muchas las que se han realizado en los últimos años. Así, la Comisión Europea la define, en su documento *Inteligencia artificial para Europa*, como aquella tecnología que, aplicada a los sistemas, hace que estos manifiestan un comportamiento inteligente, siendo capa-

25 Vid. PAZOS, A., PEDREIRA, N., RABUÑAL, J.R. y PEREIRA, J.: “Inteligencia Artificial y computación avanzada”, *Inteligencia Artificial y computación avanzada*, ROMERO, J.J., DAFONTE, C., GÓMEZ, A., PENOUSAL, F.J. (EDS.) eD. Fundación Alfredo Brañas, 2007, pág. 11

26 Vid. *AI: 15 key moments in the story of artificial intelligence*. (2020). Accesible en <https://www.bbc.co.uk/teach/ai-15-key-moments-in-the-story-of-artificial-intelligence/zh77cqt>.

27 Vid. HOCHÉL, M y GÓMEZ MILÁN, E: *La inteligencia*, 2012 pág. 35

28 Concretamente se acuñó en 1955, en la propuesta que McCarthy envió a la conferencia. Cfr. MCCARTHY, J., MINSKY, M.L., ROCHESTER, N., SHANNON, C.E., *A proposal for the Dartmouth summer research Project on artificial intelligence*, 1956

29 “En términos generales, la inteligencia artificial es el arte de elaborar de sistemas capaces de resolver problemas y desempeñar tareas mediante la simulación de procesos intelectuales.” Cfr. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (2018), *Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial*, pág. 2

ces de analizar su entorno y, con cierto grado de autonomía, pasar a la acción con determinados objetivos concretos<sup>30</sup>. El Comité Económico y Social Europeo definió a la inteligencia artificial como “*la automatización de comportamientos inteligentes como razonar, recabar información, planificar, aprender, comunicar, manipular, observar e incluso crear, soñar y percibir*”<sup>31</sup>. En la misma línea, el informe sobre la estrategia española en I+D+i en inteligencia artificial define a esta como “*la Ciencia e Ingeniería que permite diseñar y programar máquinas capaces de llevar a cabo tareas que requieren inteligencia para ser realizadas*”<sup>32</sup>.

Si la inteligencia la definía GARDNER como la capacidad de resolver problemas o generar productos que sean valiosos para una o más culturas, la inteligencia artificial podría ser definida como la disciplina científica que se ocupa de crear programas que ejecutan operaciones o toman decisiones similares a las que realiza el ser humano, como aprender o razonar de forma lógica<sup>33</sup>. Hay algunos autores que no incluyen el aprendizaje como una característica esencial de la inteligencia artificial, sino que bastaría con ampliar algunas de las capacidades relacionadas con la inteligencia natural. De este modo, BRYSON define la inteligencia artificial como aquellos “*artefactos, normalmente digitales, que amplían alguna de las capacidades relacionadas con la inteligencia natural. Así, los sistemas automáticos de visión, el reconocimiento de voz, el reconocimiento de patrones y los sistemas de producción fija, es decir, que no aprenden, se consideran ejemplos de inteligencia artificial*”<sup>34</sup>.

Especialmente didáctica es la definición aportada por BARR Y FEIGENBAUM, cuando dicen que “*la Inteligencia Artificial es la parte de las Ciencias de la computación que se ocupa del diseño de sistemas de computación inteligentes, esto es, sistemas que exhiben las características que asociamos con la inteligencia en el comportamiento humano*”<sup>35</sup>. Algunos han llegado a afirmar que la inteligencia artificial es “*el estudio de cómo lograr que los computadores realicen tareas que, por el momento, los humanos hacen mejor*”<sup>36</sup>.

---

30 Comisión Europea (2018) *Inteligencia artificial para Europa*, pág. 1 Accesible en: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF>

31 Cfr. Comité Económico y Social Europeo (2017), *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*, pág. 3

32 Cfr. Ministerio de Ciencia, Innovación y Universidades (2019), *Informe sobre la estrategia española en I+D+i en inteligencia artificial*, pág. 12

33 GARDNER, H: *Frames of Mind. The Theory of Multiple Intelligences*, Ed. Basic Books, pág. 12

34 Cfr. BRYSON, J.J.: *La última década y el futuro del impacto de la IA en la sociedad...* Op. cit., pág. 5

35 BARR, A. y FEIGENBAUM, E: *The handbook of Artificial Intelligence Volumen I* Ed. William Kaufmann, 1981, Pág. 3

36 RICH, E. y KNIGHT, K.: *Inteligencia Artificial* Mc Graw Hill 1994

PETIT se refieren a la inteligencia artificial como todas aquellas tecnologías que hacen que los ordenadores puedan llegar a desarrollar procesos cognitivos, y la subdividen en el aprendizaje automático, capaz de interpretar datos, tomar decisiones y llevar a cabo acciones para cumplir con el objetivo, y en el aprendizaje profundo, que puede gestionar grandes conjuntos de datos para generar modelos y reconocer patrones en ellos.<sup>37</sup> Algunos autores sostienen que “*la inteligencia artificial se ocupa de ampliar la capacidad de las máquinas para realizar funciones que se considerarían inteligentes si las realizaran personas*”<sup>38</sup>.

Después de analizar distintas definiciones, lo que casi todas ellas tienen en común, es la capacidad de un software para llevar a cabo alguna actividad de tratamiento de datos que lleve aparejada bien la toma de decisiones, bien una propuesta para que esas decisiones sean tomadas por humanos.

Finalizaré con el concepto dado recientemente por el Parlamento Europeo en su Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. En el citado documento, la institución europea definió la inteligencia artificial como aquel sistema “*basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la adopción de medidas, con cierto grado de autonomía, para lograr objetivos específicos*”<sup>39</sup>. Será esta, por distintos motivos, la que utilizaré en este trabajo como referencia. Primero, porque es la que ha sido tenida en cuenta por los expertos europeos a la hora de redactar la propuesta de modificación de la Directiva 85/374 de la que hablaré más tarde con profundidad. En segundo lugar, porque me parece jurídicamente la más completa y comprensible de todas las que he expuesto hasta ahora.

No quiero finalizar este apartado sin destacar, para comprender mejor la inteligencia artificial actual, dos elementos fundamentales en el avance exponencial de esta ciencia durante los últimos años: El primero, la capacidad de almacenamiento, que se ha visto incrementada de una manera muy importante y que hace que pueda tratar un número de datos ingente. El segundo, la velocidad del procesamiento de esos datos que almacena, que permite aplicaciones reales de manera casi inmediata, a través de la técnica conocida

---

37 PETIT, M.: “Por una crítica de la razón algorítmica. Estado de la cuestión sobre la inteligencia artificial, su influencia en la política y su regulación”, en *Quaderns del CAC*, n°44, 2018, pág. 5

38 PÉREZ, C.: “Inteligencia Artificial y Educación”, en *Anales de la Pedagogía*, n°7, 1989, pág. 84

39 Parlamento Europeo (2017). *Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*.

como *Big data*<sup>40</sup>. Así, en lugar de que el ordenador tenga muchas reglas predefinidas, se le programa con una serie de algoritmos -conjunto de reglas o instrucciones incluidas en un programa informático- para que aprenda todo lo posible sobre algo o alguien, para que, a su vez, en base al máximo número de datos que pueda obtener, los ordene y tome una serie de decisiones de manera autónoma en periodo muy corto de tiempo.<sup>41</sup> En muchos casos, la gran cantidad de datos y la velocidad de su análisis hacen que esta tarea sea imposible de realizar por la mente humana. Una vez más, el tratamiento de datos a gran escala se revela como un elemento fundamental en esta ciencia. A mayor número de datos, mayor acierto en las previsiones.

Por último, una vez analizado el concepto de inteligencia artificial, debo mencionar las distintas manifestaciones que esta puede tener, unas físicas y otras inmateriales. Unas, a través de un programa informático, un software al que denominaremos aplicación, y otras, incorporando ese software en elementos físicos, denominados hardware, al que se conoce como robots<sup>42</sup>. Estos últimos son más fáciles de tener presentes, pues tienen una representación física reconocible, pero no podemos obviar el estudio de aquellos programas que, aun sin tener forma física determinada, tienen tanta o más influencia en nuestra vida diaria, afectando a derechos que deben de ser protegidos igualmente<sup>43</sup>. Ambos tienen la potencialidad de causar daños a personas o a cosas y por eso los incluiré en el estudio de esta monografía.

#### 4. LA INTELIGENCIA ARTIFICIAL Y EL DERECHO. LOS RETOS ANTE LA NECESARIA ADAPTACIÓN LEGISLATIVA

El Derecho siempre ha tenido que ir adaptándose a los cambios que van surgiendo en la sociedad. Unos cambios que, como es sabido, van a mayor velocidad que esa adaptación. Como afirmaba de forma muy acertada SERRANO VILLAFÑE, “*la función del Derecho es recoger esa realidad social cam-*

---

40 Vd. CORVALÁN, J.G.: “Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia”, en *Revista de Investigações Constitucionais*, Vo.5, n°1, 2018, pág. 297

41 Vid. WRITZ, K.: “Cómo hacen Netflix y Spotify para saber lo que te gusta (sí, con inteligencia artificial)”, en *Entrepreneur*, octubre de 2018

42 Así lo señala la Comisión Europea afirmando que “los sistemas basados en la IA pueden consistir simplemente en un programa informático (p. ej. asistentes de voz, programas de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware (p. ej. robots avanzados, automóviles autónomos, drones o aplicaciones del internet de las cosas)” Cfr. Comisión Europea (2018) *Inteligencia artificial para Europa*, pág. 1

Vid. SÁNCHEZ ZAPLANA, A.: “Breve introducción a la Inteligencia Artificial para todos los públicos”, en *El Consultor de los Ayuntamientos*, n°10, octubre 2019

43 MIRÓ LLINARES, F.: “Inteligencia artificial y justicia penal: Más allá de los resultados lesivos causados por robots”, en *Revista de Derecho Penal y Criminología*, 3° Época, n.º 20, 2018, pág. 89

*biante y regular sus múltiples relaciones jurídicas con fines de seguridad, certeza, y bien común, que son fines del Derecho*<sup>44</sup>.

Pero esos habituales cambios, y las necesarias adaptaciones correspondientes, están marcados hoy por dos elementos que hacen aún más compleja la respuesta del mundo legal, ya de por sí parsimoniosa, como son la rapidez con que se producen y la magnitud de los mismos. El avance de la tecnología en general, y de la inteligencia artificial en particular, no es lineal, sino exponencial, lo que supone un reto para el mundo del Derecho y los legisladores<sup>45</sup>.

Sirva de ejemplo precisamente el caso de estudio de esta monografía. Hace ya años que los robots dotados con inteligencia artificial son comercializados en Europa. Desde los vehículos a motor que pueden realizar determinadas tareas de manera autónoma, como frenar cuando se encuentra a cierta distancia de un objeto o cambiar el tipo de luces, hasta los más simples robots que son capaces de limpiar superficies sin necesidad de la acción del hombre. Pues bien, mientras ese cambio social llegaba a nuestro día a día, no fue hasta 2017 cuando el Parlamento Europeo, como ya hemos señalado, se planteó la necesidad de una reforma legal en este ámbito que no llegará, siendo muy optimista, hasta dentro de uno o dos años. En el mismo sentido se ha pronunciado en diferentes ocasiones la Comisión Europea al sostener que es necesario revisar el marco jurídico tanto nacional como europeo para adaptarlo a estos nuevos tiempos.<sup>46</sup> Esa voluntad de cambio legislativo ha sido también asumida por el gobierno de España, al incluir en su estrategia sobre inteligencia artificial los aspectos legales y regulatorios de la inteligencia artificial, afirmando que se *“requiere de un marco legal adaptado para que la IA se utilice de manera justa, transparente y responsable”*<sup>47</sup>.

Esto quiere decir que los operadores jurídicos deberán aplicar normas que no están adaptadas a esta nueva realidad, algunas de ellas con décadas a sus espaldas como la relativa a la responsabilidad por productos defectuosos recogida en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios de 2007. Es cierto que ello tiene su sentido, porque los cambios en las normas tienen que ser bien meditados y, en la medida de lo posible, con un horizonte de permanencia y validez lo más amplio posible.

---

44 Cfr. SERRANO VILLAFañE, E., “Funciones del Derecho en la sociedad cambiante de nuestros días”, en *Anuario de Filosofía del derecho*, n°17, 1974, pág. 472

45 Como afirma BARRIO ANDRÉS *“los robots y los sistemas de inteligencia artificial son uno de los grandes inventos verdaderamente disruptivos del entorno digital, y constituyen, sin duda, un vector de cambio vertiginoso de nuestras sociedades que apenas si hemos comenzado a vislumbrar.”* Cfr. BARRIO ANDRÉS, M.: “Robótica, inteligencia artificial y Derecho”, en *Análisis del Real Instituto Elcano*, n°113, 2018, pág. 3

46 Comisión Europea (2018), *Coordinated Plan on the development and use of Artificial Intelligence Made in Europe*, pág. 3

47 Vid. Ministerio de Ciencia, Innovación y Universidades (2019), *Informe sobre la estrategia...*, Op.cit. pág. 40

No se puede legislar al albur de un acontecimiento concreto o impactante, o por la aparición de una nueva tecnología, sino que se ha de hacer con profundidad jurídica para evitar la aprobación de leyes que adolezcan de la calidad necesaria para afrontar los problemas o cuestiones que intentan atajar. Como señala PALMERINI, “*sigue siendo válida la enseñanza según la cual todo fenómeno nuevo, especialmente cuando está ligado al desarrollo científico y tecnológico, no requiere necesariamente de la introducción de normas nuevas, ante la posibilidad de ser regulado por el sistema existente, capaz de adquirir una gran elasticidad*”<sup>48</sup>.

Esta circunstancia no es una novedad en nuestro Derecho. Es más, es muy habitual. Pero para ello también hay respuesta, gracias a la evolución jurisprudencial que puede ir, en la medida de sus posibilidades y con evidentes limitaciones, adaptando la realidad social a la resolución de conflictos jurídicos. Baste pensar que a principios del siglo XX no existía legislación específica en materia de protección al honor, y no la hubo hasta la Ley de 1982, cuando el Tribunal Supremo, en 1912, introdujo el concepto de honra y emitió la primera sentencia condenatoria, en este caso por la publicación de una noticia inveraz respecto a un fraile y una joven del municipio murciano de Totana.

Pero nos encontramos ante un cambio de tal magnitud que, sin duda, hará que modifiquemos nuestra legislación en distintas áreas. Así, en los próximos años asistiremos a reformas en el ámbito del Derecho laboral, del tributario y, por supuesto, del civil. Tanto es así que el Parlamento Europeo, como más tarde analizaré, ha presentado a la Comisión Europea una propuesta para la modificación de la Directiva 85/374. Hay que dar solución a preguntas relativas a cómo responder, por ejemplo, ante los daños que pueda provocar la inteligencia artificial o cómo proteger nuestra privacidad ante un uso masivo de datos para distintos fines. Una adaptación necesaria que ha de realizarse teniendo como base las leyes ya existentes, incorporando novedades que protejan a los consumidores y usuarios, pero que también permitan el desarrollo económico y social de la técnica que marcará las próximas décadas, y de los operadores del sector, que deben de conocer las reglas para adaptarse así a las mismas. De lo que no cabe duda, como como ahora he señalado, es que estas reformas legislativas forman parte de la agenda política de distintos países y de la propia Unión Europea, que lleva años trabajando en este sentido.

Por lo que respecta a la preocupación del Derecho por la inteligencia artificial, ésta no es tan reciente como podría pensarse. Ya en los años 70 se publicaron los primeros trabajos jurídicos en referencia a ella<sup>49</sup>. Fueron

---

48 PALMERINI, E.: “Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea”, en *Revista de Derecho Privado*, nº32, 2017, pág. 60

49 Una completísima bibliografía de esa década sobre Derecho y nuevas tecnologías puede consultarse en

“Computer-Assisted Legal Research Bibliography, 1 Computer”, en *Computer and Law Journal*, Vol.1, 1978

BUCHANANT Y HEADRICK los que publicaron el conocido trabajo *Some Speculation About Artificial Intelligence and Legal Reasoning* en el que reclamaban que el mundo jurídico aprovecharse la potencialidad de la inteligencia artificial para su trabajo e investigación, si bien no entraban en temas como la responsabilidad o la propiedad intelectual<sup>50</sup>. En el año 1971 la revista *Law Library Journal* publicó un número monográfico sobre el Derecho y las Nuevas Tecnologías en las que ya aparecían temas relacionados con la inteligencia artificial<sup>51</sup>. En España, PÉREZ LUÑO fue pionero en el estudio de la relación del Derecho con la Informática, a través de su obra *Cibernética, Informática y Derecho*<sup>52</sup>.

Pero esa preocupación original del Derecho sobre las nuevas tecnologías se ha de transformar en la toma de decisiones en el ámbito legislativo. Como señala el informe *Inteligencia Artificial desde una perspectiva europea*, las oportunidades que ofrece la inteligencia artificial son muchas, pero también lo son los desafíos que esta presenta<sup>53</sup>. No cabe duda de que uno de esos desafíos es el de las modificaciones legales necesarias, de las que hablaré con detalle en esta monografía, al menos, en lo que respecta al derecho civil.

Sin ánimo de ser exhaustivo, puesto que posteriormente trataré el tema con mayor profundidad, basta con examinar la actuación de las instituciones europeas en esta materia relacionada con el Derecho civil en los últimos años para darse cuenta de que ya estamos inmersos en ese proceso profundo de cambio legislativo. En 2017 el Parlamento Europeo emitió un informe con recomendaciones destinadas a la Comisión Europea sobre normas de Derecho civil en materia de robótica<sup>54</sup>. En el mencionado informe se solicitaba a la Comisión Europea que adoptase medidas, principalmente, respecto a la responsabilidad civil y la conducta ética en este ámbito, sobre el que posteriormente profundizaré. Meses después, el propio Parlamento Europeo abrió una consulta pública para debatir acerca del futuro de la robótica

---

<sup>50</sup> Señalaban algo que casi cuatro décadas después es ya una realidad: “*que la investigación jurídica en informática podría mejorar nuestra comprensión de los procesos por los que los abogados trabajan y piensan. Hasta ahora los abogados no han intentado explorar su relevancia. Deberían*”

BUCHANANT B.G. y HEADRICK, T.E.: “Some Speculation About Artificial Intelligence and Legal Reasoning”, en *Stanford Law Review*, Vol. 23, n°1, 1970, pág. 62

<sup>51</sup> Cfr. *Law Library Journal*, Vol 64, n°2, 1971

<sup>52</sup> Pérez Luño, A. E.: *Cibernética, Informática y Derecho. Un análisis metodológico*, Ed. Publicaciones del Real Colegio de España, 1976

<sup>53</sup> Comisión Europea (2018), *Inteligencia artificial desde una perspectiva europea*, pág. 23. Accesible en : <https://ec.europa.eu/jrc/en/publication/artificial-intelligence-european-perspective>

<sup>54</sup> Parlamento Europeo (2017). *Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*. [online] Mady Delvaux. Available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//ES> [Accessed 10 Jan. 2018].

y la inteligencia artificial, centrándose principalmente en lo que atañe al Derecho civil<sup>55</sup>.

En el año 2018, la Comisión Europea creó un Grupo de Expertos sobre responsabilidad y nuevas tecnologías, del que he tenido la oportunidad de formar parte como suplente, y cuyo trabajo se ha traducido en recomendaciones sobre el sistema de responsabilidad civil en el ámbito de la inteligencia artificial y la necesaria modificación de la Directiva del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos sobre la que más tarde profundizaremos<sup>56</sup>. Como ya he comentado, un informe del Parlamento fechado el pasado año 2020, va más allá y propone la modificación de la Directiva 85/374 para adaptarla a los nuevos retos de la inteligencia artificial convirtiéndola en un Reglamento Europeo que homogenice el sistema de responsabilidad civil en todos los países miembros de la Unión Europea.

Pero no solo la Unión Europea ha alertado sobre la necesidad de realizar las correspondientes modificaciones legislativas. El Gobierno de Estados Unidos elaboró el año 2016 un informe en el que aparecen los principales retos y riesgos de la Inteligencia Artificial. En el documento *Preparing for the Future of Artificial Intelligence*<sup>57</sup>, se muestra la necesidad de regular los aspectos legales de la Inteligencia Artificial, especialmente en lo relativo a los vehículos autónomos. Tanto es así, que el 7 de septiembre de 2017 Estados Unidos aprobó la *Self Drive Act*, primera ley en la que se regulan las condiciones de circulación de los vehículos autónomos<sup>58</sup>. En nuestro país, el Director General de Tráfico ya anunció que se trabaja en una Ley del coche autónomo, que, aunque preveía ser aprobada el pasado 2018, aún no ha pasado el trámite legislativo correspondiente<sup>59</sup>.

---

55 La mencionada consulta se produjo entre el 8 de febrero y el 1 de junio de 2017, y sus resultados se pueden consultar en <http://www.europarl.europa.eu/cmsdata/130980/comision-asuntos-juridicos-resumen-consulta-robotica.pdf>

56 Toda la información sobre el citado grupo y sus trabajos se pueden encontrar en el siguiente enlace: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592>

57 Executive Office of the President National Science and Technology Council Committee on Technology (2016). *Preparing for the Future of Artificial Intelligence*. [online] Available at: [https://obamawhitehouse.archives.gov/sites/default/files/whitehouse\\_files/microsites/ostp/NSTC/preparing\\_for\\_the\\_future\\_of\\_ai.pdf](https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf) [Accessed 10 Jan. 2018].

58 La ley puede consultarse en <https://www.congress.gov/bill/115th-congress/house-bill/3388>

59 “La DGT adaptará la ley al coche autónomo después de conocer la opinión del sector.”, en *El faro de Vigo*, 6 de diciembre de 2017. Accesible en: <http://www.farodevigo.es/economia/2017/12/06/dgt-adaptara-ley-coche-autonomo/1798783.html>

Es un hecho, por lo tanto, que los principales actores internacionales han comenzado ya a trabajar para encontrar la mejor manera de afrontar los retos jurídicos, económicos y éticos relacionados con la inteligencia artificial. En esta monografía trataré de analizar en qué punto nos encontramos y hacia dónde se dirige la legislación en materia de Derecho civil relativa a la Inteligencia Artificial.

Uno de los elementos sobre el que deberá girar gran parte de la futura legislación es la capacidad que puede tener la inteligencia artificial para tomar decisiones de manera autónoma sin la participación directa del ser humano. Y digo directa porque, evidentemente, el hecho de haber creado el software necesario para poder llegar a ese punto no deja de ser, de forma indirecta, una forma de participación por parte del hombre. Como señala MIRÓ LLINARES, “*la autonomía de una IA provendría de la capacidad real de adaptar las decisiones a un contexto distinto de aquél para el que ha sido programada*”<sup>60</sup>.

Hay, por lo tanto, cierto consenso en la doctrina en que la aparición de la inteligencia artificial ha generado nuevos desafíos a los que no se puede hacer frente con la regulación jurídica actual<sup>61</sup>. Es cierto que no todo cambio en el ámbito tecnológico exige un cambio profundo de legislación, puesto que son muchos los casos en los que la normativa preexistente da respuesta a los nuevos desafíos generados. Pero, como ya he comentado anteriormente, las instituciones internacionales y europeas ya han dado los primeros pasos para las modificaciones legislativas que se adapten a la irrupción en nuestro día a día de la inteligencia artificial. Una opinión que comparto puesto que, a pesar de la razonable respuesta que ha venido dando la legislación actual, es necesario llevar a cabo una serie de reformas legales a nivel internacional y nacional para poder aportar seguridad jurídica tanto a los operadores como a los ciudadanos. Un marco jurídico que permita compatibilizar los avances de la tecnología en el ámbito de la inteligencia artificial con los derechos y la seguridad de los ciudadanos. Una nueva legislación que dé respuesta a cuestiones complejas como la responsabilidad civil o la privacidad, entre otros muchos aspectos que se ven afectados de manera muy directa por los avances en esta materia<sup>62</sup>.

---

60 MIRÓ LLINARES, F.: “Inteligencia artificial y justicia penal... Op.cit., pág. 93

61 Entre otros muchos: BARRIO ANDRÉS, M.: “Robótica, inteligencia artificial y Derecho... Op.cit., pág. 4

62 Sostiene en este mismo sentido PALMIERI que “*entre las circunstancias que justifican un tratamiento unitario del tema, al menos prima facie, se encuentra, principalmente, una cuestión fáctica, esto es, el hecho de que las múltiples aplicaciones estudiadas pertenecen a un mismo sector de la investigación y de la innovación tecnológica -la robótica- que, aunque se vale de diversas disciplinas para poner en funcionamiento sus productos, presenta características suficientemente específicas y propias. En segundo lugar, la relevancia es de carácter socioeconómico, puesto que la robótica implica un mercado en expansión, considerado estratégico sobre el plano económico y de gran impacto a nivel social, cuyo crecimiento requiere ser controlado mediante una intervención regulatoria.*” Cfr. PALMIERI, E., “Robótica

Hay algunos autores que van aún más allá y proclaman, no solo la necesidad de regular de manera específica aquellas materias relacionadas con la inteligencia artificial, sino que hablan del nacimiento de una nueva disciplina: el Derecho Artificial o Derecho de los robots<sup>63</sup>. Yo soy más partidario de englobarlo en un área algo más amplia, la del Derecho de las nuevas tecnologías, que abarca más contenido y permite mayor flexibilidad y adaptación a las novedades que vayan surgiendo, que no serán pocas, en los próximos años.

No podremos tampoco olvidar un elemento muy relacionada con la inteligencia artificial, que son los datos. La combinación de la primera con estos últimos es una herramienta muy potente, deseada por su alto valor económico, tendrá una incidencia elevada en la intimidad de todos los ciudadanos.

---

y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea”, *Revista de Derecho Privado*, n° 32, enero-junio de 2017, Pág. 55

63 Define CANALS AMETLLER esta nueva disciplina “*como conjunto de principios y reglas jurídico-técnicas que ordenen las situaciones y las relaciones en las que concurre un objeto artificial o inhumano con capacidad física y mental*” Cfr. CANALS AMETLLER, D.: “El proceso normativo ante el avance tecnológico y la transformación digital (Inteligencia artificial, redes sociales y datos masivos)”, en *Revista General de Derecho Administrativo*, n° 50, 2019, pág. 3

BARRIO ANDRÉS, M.: “Robótica, inteligencia artificial y Derecho... Op.cit., pág. 6



## CAPÍTULO II

# INTELIGENCIA ARTIFICIAL, ROBOTS Y PERSONALIDAD JURÍDICA

### 1. CONCEPTO DE ROBOT

Como previamente comentábamos, la inteligencia artificial puede aparecer en una aplicación informática sin representación física alguna, o incorporándose a un elemento físico, conocidos como robots. A lo largo de este capítulo intentaré determinar si existe o no la necesidad de dotar a estos robots de algún tipo de personalidad, como proponen algunos sectores de la doctrina.

Antes de entrar de lleno en el complejo tema de la personalidad, es necesario hacer una breve introducción a cerca del concepto básico de robot. La denominación actual procede del término checo *robota*, que significa trabajador o siervo, y fue acuñado a principios del siglo XX por el escritor checo Karel Capek<sup>64</sup>. Si bien es cierto que el origen de los robots se sitúa en la primera mitad del siglo XX, usados básicamente para la realización de tareas industriales de la época, fue a partir de la aparición de los ordenadores personales cuando estos comenzaron a llevar a cabo tareas de manera autónoma, cuyo desarrollo y perfeccionamiento se produjo ya en los primeros años del siglo XXI<sup>65</sup>.

Los robots más conocidos por todos nosotros venían siendo los industriales, esos a los que me acabo de referir, cuyo uso principal era llevado a cabo en distintos procesos de fabricación. También han adquirido recientemente

---

64 A este origen se refiere GUARDIOLA SALMERÓN, situándolo en la obra del escritor *Los robots universales de Rossum*, 1920. Vid. GUARDIOLA SALMERÓN, M.: “Robótica e inteligencia artificial: nuevos desafíos jurídicos”, en *Law & Trends*, julio 2016, <https://www.lawandtrends.com/noticias/tic/robotica-e-inteligencia-artificial-nuevos.html>

65 GARCÍA-PRIETO señala hasta nueve tipos de robots según su aplicación: Contesto ambiental, cirugía, prostética, salud y calidad de vida, militar, educación, juguetes, entretenimiento y arte. Vid. GARCÍA-PRIETO CUESTA, J.: “¿Qué es un robot?”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluwer, pág. 30 a 45

un papel muy importante aquellos destinados a usos militares, de investigación espacial o incluso para actuaciones de la administración pública. Baste señalar que, durante la pandemia del COVID19, algunas administraciones como la Junta de Andalucía, han utilizado robots para resolver en tiempo récord las miles de solicitudes de ayudas recibidas<sup>66</sup>. En la actualidad, se abren paso los denominados robots domésticos, cuya misión es hacernos la vida más fácil a los humanos, y los robots en el ámbito sanitario<sup>67</sup>. Es cierto que no todos ellos serán robots inteligentes, puesto que muchos de ellos se limitarán a ser tan solo automáticos -especialmente del sector industrial- y otros carecerán de esa *inteligencia* o capacidad de interpretar datos o tomar decisiones autónomas, como muchos de los robots utilizados en la medicina para la realización de operaciones, que son manejados a través de una especie de consola por los profesionales de la medicina o los propios drones de uso militar que, aunque carezcan de piloto en el aparato, cuentan con uno de forma remota. No obstante, trataré de analizar la problemática de los robots centrándome en aquellos que realizan sus tareas a través de técnicas que incluyan la inteligencia artificial de uno u otro modo.

La RAE define al robot como la “*máquina programable capaz de realizar trabajos antes reservados solo a las personas.*” Una definición que, aunque muy básica, nos puede servir bien para comprender una de las principales problemáticas que han surgido en estos años. Los robots han ido aumentando de forma exponencial el número de tareas que son capaces de hacer y que antes tan solo el ser humano podía llevar a cabo. De este modo, han comenzado a surgir debates sobre su papel tanto en el ámbito civil, a la hora principalmente de determinar la responsabilidad civil, como en el laboral y fiscal, en los que surgen dudas acerca de la conveniencia de considerar a los robots como trabajadores y así ser sujetos de obligaciones fiscales. Sobre esta materia, din duda interesante, la doctrina, como ahora veremos, no se llega a poner de acuerdo.

Pero es necesario profundizar algo más en un concepto actual que nos permita afrontar el estudio de la necesidad de dotar de personalidad o no a los robots. Así, GARCÍA-PRIETO sostiene que los robots son “*un mecanismo complejo que interactúa con su entorno, ejercitando una cierta complejidad*”

---

66 Andalucía usará robots para dar ayudas de 1.000€ a 80.000 autónomos en dos meses. El Confidencial, 18 de noviembre de 2020. Accesible en [https://www.elconfidencial.com/espana/andalucia/2020-11-18/andalucia-usara-robots-ayudas-autonomos\\_2836644/](https://www.elconfidencial.com/espana/andalucia/2020-11-18/andalucia-usara-robots-ayudas-autonomos_2836644/)

67 Acerca de estos últimos, PALMIERI da muchos detalles al afirmar que “*los robots quirúrgicos implementados actualmente en los hospitales, y entre sus objetivos más prometedores, todavía objeto de experimentación, la elaboración de cápsulas médicas inteligentes para llegar a sitios del interior del cuerpo humano; terapia motora, mental, cognitiva y social, asistida robóticamente; sistemas de monitoreo de parámetros fisiológicos robotizados y prótesis biónicas avanzadas implantadas directamente en el sistema nervioso central o periférico.*” Cfr. PALMIERI, E., “Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea”, *Revista de Derecho Privado*, n° 32, enero-junio de 2017, Pág. 53

(desarrollando un comportamiento difícil de predecir), suficiente como para que, en algunos casos, sea capaz de sustituir a un ser humano en algunas de las tareas que realiza, especialmente en un entorno dinámico y cambiante”<sup>68</sup>. En el mismo sentido, SANTOS GONZÁLEZ define el robot inteligente como la “máquina física que de manera autónoma a través de programas y sensores inteligentes pueda llegar a tomar decisiones basándose en la lógica e inteligencia artificial prediciendo las necesidades de los humanos y de las situaciones en las que se ven envueltos actuando, alterando e interactuando con el mundo físico, todo ello sin estar sometidos al control continuo de los humanos”<sup>69</sup>. Ambas definiciones ponen de manifiesto dos elementos que se van a demostrar fundamentales. Por un lado, el comportamiento difícil de predecir de los robots y que conlleva interacción en el entorno de este. Y, por otro, un elemento esencial cual es la existencia de cierta autonomía a la hora de tomar decisiones por parte de los robots, independientes algunas de ellas del ser humano. Posteriormente volveré sobre esta cuestión para tratarla con mayor detenimiento puesto que esa autonomía en la toma de decisiones tiene su raíz en la programación que lleve a cabo el ser humano.

El Parlamento Europeo, en su informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, establece las características de los robots dotados de inteligencia artificial<sup>70</sup>. En primer lugar, lo que diferencia a los robots inteligentes del resto de la inteligencia artificial es que se trata de un elemento físico. Esta circunstancia es tremendamente relevante pues, a los riesgos de cualquier software que también van a estar presentes en los robots, hay que sumarles los que pueden generarse por el hecho de ser un ente físico. En segundo lugar, deben de tener “capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno y el intercambio y análisis de dichos datos.” Es decir, ser capaces de tomar decisiones sin la participación del ser humano o, mejor dicho, tan solo con los algoritmos introducidos por este con carácter previo. La tercera de las características señaladas por el informe del Parlamento Europeo es la “capacidad de autoaprendizaje a partir de la experiencia y la interacción”. Igualmente, en cuarto lugar, han de ser capaces de poder adaptar sus actuaciones al entorno en el que se encuentren. Por último, como es evidente, los robots no pueden tener vida en sentido biológico, puesto que en tal caso nos encontraríamos ante una persona física.

A los robots también se refiere BARRIO atribuyéndoles tres características esenciales. La primera a la que hace mención es la capacidad de vigilar el entorno y detectar los cambios que en él se produzcan, operación que

---

68 Vid. GARCÍA-PRÍETO CUESTA, J.: “¿Qué es un robot?”, *Derecho de los robots...* Op. cit, pág. 38

69 SÁNTOS GONZÁLEZ, M.J.: “Regulación legal de la robótica y la inteligencia artificial: Retos de futuro”, en *Revista Jurídica de la Universidad de León*, n° 4, 2017, pág. 32

70 Cfr. Parlamento Europeo (2017), *Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*, págs. 8 y 9

se realiza a través de sensores. La segunda es la inteligencia artificial, que es la que determina como va a responder el robot. Y la tercera y última, la de actuar provocando algún tipo de cambio en ese entorno<sup>71</sup>. Todas estas características me permiten centrar el tema tratando de responder una simple cuestión: ¿Un ente como los robots, con los elementos ahora señalados, debe de tener algún tipo de personalidad? Y de ser ello viable, ¿Aportaría algún tipo de solución al que no se podría llegar sin la atribución de la mencionada personalidad?

## 2. LA PERSONALIDAD JURÍDICA

Es también necesario, con carácter previo al estudio de la posibilidad de dotar de personalidad a los robots, tratar de determinar brevemente el concepto general de esa personalidad. Ello me lleva a concretar inicialmente el concepto de persona, y por qué podemos hablar de clases de personas<sup>72</sup>. La etimología primitiva de la palabra persona parte del escenario de la Roma Clásica, en el teatro, donde los personajes que representaban los papeles en las obras utilizaban una máscara denominada personare, en el que tiene su origen este concepto; fue de ahí de donde pasó a tener ya un significado jurídico<sup>73</sup>.

No entraré en mayor profundidad sobre el concepto de persona física, puesto que la posible atribución de personalidad a los robots nunca podría ir aparejada a esta, sino, en cualquier caso, a la persona jurídica. Pero no quiero dejar de recordar algo esencial como es el hecho de que la persona física la considera el Derecho como sujeto de derecho, es decir, sujeto de la relación jurídica y sujeto del derecho subjetivo y del deber jurídico<sup>74</sup>. Una circunstancia elemental, y que será recurrente a lo largo del trabajo, es que la única razón que tiene el derecho de existir es el ser humano y, especialmente, las relaciones entre estos.

La persona jurídica, en cambio, como señalaba COSSIO, tiene sus raíces en la doctrina política de los filósofos griegos y en la jurisprudencia romana que dan origen a esta forma de subjetividad colectiva, que aparecen como complejos de relaciones y no como personas<sup>75</sup>. Luego volveré sobre esta ma-

71 BARRIO ANDRÉS, M.: *Derecho de los Robots...* Op. cit. pág. 70

72 Esta breve introducción sobre el concepto de persona es una adaptación de mi anterior trabajo "La capacidad de las menores de edad, mayores de 16 años, para abortar", *Políticas jurídicas para el menor*, SAINZ-CANTERO CAPARRÓS, M.B. (Dir.), Ed. Comares 2010, págs. 75 y ss.

73 Vid. BETANCOURT, F. *Derecho Romano Clásico*. Ed. Universidad de Sevilla, 2007. Pág. 51

74 Vid. O'CALLAGHAN MUÑOZ, X.: *Código Civil Comentado y con Jurisprudencia*. Ed. La Ley, Madrid 2008. Pág. 82

75 COSSIO CORRAL, A.: "Hacia un nuevo concepto de la persona jurídica", en *Anuario de Derecho Civil*, 1954, pág. 638

teria, que ya adelanto fundamental para la resolución de la cuestión, puesto que un elemento básico de las personas jurídicas, que no encontraremos en los robots, es que se fundamenta en la existencia de una colectividad formada por personas físicas, con un objetivo común.

Nuestra doctrina ha analizado a lo largo de la historia profusamente el concepto jurídico de persona. Así, PUIG BRUTAU la define como “*el individuo o ser humano capaz de derechos y obligaciones; o, si se quiere, como sujeto activo o pasivo de una relación jurídica*”<sup>76</sup>. En el mismo sentido, CASTÁN sostenía que “*persona es todo ser capaz de derechos y obligaciones, es decir, es el sujeto, activo o pasivo, de relaciones jurídicas*”<sup>77</sup>. Quisiera resaltar la importancia de esto último, la capacidad de toda persona jurídica de ser titular de derechos y obligaciones. Y lo hago porque será uno de los principales argumentos en el que me apoyaré para negar, lo adelanto ya, la posibilidad de que los robots puedan tener personalidad jurídica sin ser titulares de derechos y obligaciones.

Me gustaría subrayar también el concepto aportado por O’CALLAGHAN, por certero y relacionado con el tema que más adelante trataré. El catedrático y magistrado emérito del Tribunal Supremo defiende que “*la persona es el ser humano –individualmente considerado como persona física o socialmente unido como persona jurídica– el Derecho lo considera como sujeto de derecho: sujeto de una relación jurídica y sujeto del derecho subjetivo y del deber jurídico*”.<sup>78</sup>

Me quiero quedar con el hecho de que es, en cualquier circunstancia, el ser humano, bien individualmente considerado o socialmente unido, el centro de la persona física, en el primer caso, y de la persona jurídica, en el segundo. Y es relevante porque, como más tarde defenderé y ahora adelanto brevemente, será otro de los argumentos para rechazar la posibilidad que algunos autores defienden para que los robots puedan tener la consideración jurídica de persona, aunque sea creando una tercera clase, la persona electrónica.

Pero hemos de diferenciar aquél sujeto individual que puede ser objeto de esos derechos u obligaciones, al que se denomina persona física, de la que se designa como persona jurídica, entendiéndose como tal aquellas agrupaciones que actúan como entidades vivas en todas las facetas de la vida social y que, aun funcionando de forma independiente de sus comportamientos personales, son dirigidas por personas físicas, a las que se les atribuye por el ordenamiento jurídico cierta capacidad. ALBALADEJO define a la persona jurídica como “*la organización humana encaminada a la consecución de un fin a la que el Derecho acepta como miembro de la comunidad otorgándole capacidad*

76 Cfr. BRUTAU, P.: *Fundamentos de Derecho Civil*. Ed. Bosch, Barcelona 1988.

77 CASTÁN TOBEÑAS, J.: *Derecho Civil Español Común y Foral*; Tomo II Vol. I, Ed. REUS, 1995

78 O’CALLAGHAN MUÑOZ, X.: *Compendio de Derecho Civil*. Tomo I Parte General. Ed. Revista de Derecho Privado. 1997

*jurídica*”<sup>79</sup>. Así, entre ellas, podremos clasificarlas por el ámbito de pertenencia -públicas o privadas-, por su estructura -asociaciones o fundaciones-, y por el interés que persiguen -ya sea público o privado-. DE CASTRO puntualiza en este sentido que “*más exacto que hablar de clases de personas sería hablar de persona sólo para la persona física, y de realidades sociales personificadas a la que se atribuye personalidad para la persona jurídica*”<sup>80</sup>.

Mucho se ha escrito sobre las diferentes teorías relativas a la persona jurídica. Así, encontramos la teoría de la ficción jurídica, nacida en Roma, en la que el ser humano es el único sujeto de derecho y la persona jurídica no es más que una ficción cuyo objetivo se limita a permitir que los colectivos de personas puedan formar parte del tráfico jurídico. Por otro, está la teoría de la voluntad, que defiende que la colectividad tiene una voluntad diferenciada de la de sus miembros. Igualmente, la teoría del interés, en la que la persona jurídica es tan solo una construcción jurídica con una intencionalidad única y exclusivamente práctica. La teoría de la institución, que defiende que se trata de una institución con unos fines determinados y es en torno a ella que se reúnen personas físicas interesados en cumplir con esos fines. Por último, la más reciente construcción lógica, que por el contrario limita a la persona jurídica a una simple técnica del lenguaje jurídico necesaria única y exclusivamente para hacer más sencilla la tarea de los operadores jurídicos<sup>81</sup>.

### 3. LA PERSONALIDAD DE LOS ROBOTS

Sin duda, uno de los temas de los que más se ha hablado y escrito a cerca de los robots es sobre su personalidad que, desde el punto de vista jurídico, podrían llegar a tener. En Europa es un debate que tiene ya un largo recorrido y cierta importancia. De este modo, la Comisión Europea financió el proyecto *Robolaw* con la intención de realizar un informe con las principales cuestiones éticas y legales de los robots en los que ya se abordaba el tema de su personalidad<sup>82</sup>. La responsable del informe, la profesora PALMERINI, de la Scuola Superiore San't Anna, analizó brevemente esta problemática, a la que ahora me referiré<sup>83</sup>.

79 Vid ALBADALEJO, M.: *Curso de Derecho Civil I* Ed. Barcelona, 2005

80 Cfr. DE CASTRO Y BRAVO, F.: *Derecho Civil de España*, Tomo II, Ed. Aranzadi 2008. Pág. 34

81 Para un estudio detallado de las teorías de las personas jurídicas: Vid FERRARA, F.: *Teoría de las Personas Jurídicas*, Ed. Comares, 2006

82 PALMERINI, E. (2014), *The RoboLaw Project: A European perspective on the ethical and legal implications of social robots*

83 La propia PALMERINI define este proyecto como “*una colaboración entre juristas e ingenieros; inicialmente estuvo focalizada en el análisis de casos de estudio individuales y, sucesivamente, adopto una postura abierta a la consideración de todas las potencialidades, aunque también de los riesgos,*

Esta cuestión también llegó también hace años, concretamente en octubre de 2013, al Parlamento Europeo a través de una pregunta del eurodiputado Marc Tarabella en la que solicitaba información sobre el estatus legal de los robots<sup>84</sup>. La contestación de la entonces vicepresidenta, la Sra. Kroes, negaba esta posibilidad puesto que “*la tecnología aún no está lista para ofrecer el grado de autonomía para otorgar personalidad o estatus legal a los robots*”<sup>85</sup>. Luego profundizaré sobre este particular, pero no creo que la personalidad dependa del mayor o menor grado de autonomía que puedan llegar a tener los robots, sino de otras circunstancias, eminentemente prácticas. A pesar de la respuesta negativa de la comisaria, como posteriormente se pudo ver, no se trataba de una negativa a futuro. Dos años más tarde, en 2015, El propio Parlamento Europeo creó un grupo de trabajo, cuyas conclusiones fueron aprobadas en enero de 2017, que planteó a la Comisión Europea la realización de un análisis en profundidad sobre la posibilidad de “*crear a largo plazo una personalidad jurídica específica para los robots*”<sup>86</sup>. Dicha propuesta de estudio no ha sido admitida por parte de la Comisión Europea, pero sí que el debate sobre la cuestión ha ido en aumento, y existe cierta división entre los expertos sobre la conveniencia de llegar a implantar esta personalidad, tema sobre el que ahora me detendré.

Pero no todas las instituciones han abierto la puerta a la posibilidad de otorgar algún tipo de personalidad legal a los robots. Así, el Comité Económico y Social Europeo se mostró en 2017 contrario a otorgar estatuto legal alguno a cualquier sistema que cuente con inteligencia artificial porque, según afirmaba en su dictamen *Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad*, “*socavaría los efectos correctores preventivos de la legislación en materia de responsabilidad, generaría un riesgo moral tanto en el desarrollo como en la utilización de la IA y daría lugar a un posible uso indebido*”<sup>87</sup>. El dictamen, en este punto, anticipaba algunas conclusiones interesantes que comparto, como el riesgo que podría suponer en el ámbito de la responsabilidad otorgar personalidad a los robots. Básicamente en lo que hace referencia a la posibilidad

---

generados por el progreso de la investigación y por los avances de la industria robótica.” Cfr. PALMERI-NI, E.: “Robótica y derecho: sugerencias, confluencias... Op. cit., pág. 62 y 63

84 TARABELLA, M. (2013), accesible en <https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2013-011289+0+DOC+XML+V0//EN>

85 KROES, N. (2013), accesible en <https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-011289&language=EN>

86 Cfr. Parlamento Europeo (2017), *Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*, pág. 20

Un análisis pormenorizado sobre el proceso de redacción del informe sobre las normas de Derecho civil sobre robótica puede consultarse en la obra de SÁNCHEZ DEL CAMPO REDONET, A.: “Europa quiere regular a los robots”, en *Diario la Ley*, n°4, 2017

87 Cfr. Comité Económico y Social Europeo (2017), *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*, pág. 2

de limitar la responsabilidad a los propios robots, eximiendo o relajando la de los operadores o fabricantes de los mismos. En el último capítulo de esta monografía analizaré este aspecto con mayor detalle.

La doctrina en este tema se encuentra dividida entre aquellos que mantienen que hay que dotar a los robots de una personalidad jurídica específica y los que, por el contrario, defienden que los robots son meros objetos y que se han de encuadrar dentro de las cosas en el Código civil. De lo que no existe duda es de que, si el Derecho existe, es única y exclusivamente por el ser humano y para regular su relación con otros iguales. Por lo tanto, el centro de la personalidad, tanto física como jurídica, será el ser humano y no los robots. En el hipotético caso de que fuese conveniente dotar a estos de personalidad, lo debería ser única y exclusivamente pensando en las bondades que podría conllevar en la relación entre los seres humanos, y no en el hecho de que los robots “*necesiten*” contar con una personalidad. Como sostendré ahora, no encuentro razón práctica alguna para respaldar la teoría de que se dote de personalidad jurídica a los robots.

### 3.1. ¿Hacia una personalidad electrónica?

Comenzaremos analizando la posibilidad de crear una nueva personalidad, la personalidad electrónica o, como algunos autores prefieren denominarla, personalidad robótica<sup>88</sup>. Si bien es una postura minoritaria entre la doctrina, alguno de los autores que la defienden sostienen que el debate no debería circunscribirse únicamente a los robots con inteligencia artificial, sino a todos ellos. Una parte de la doctrina aboga por incluir a los robots en la ya existente realidad de la personalidad jurídica. Así esta línea doctrinal sostiene que, aunque los robots no deben tener la misma condición de persona física que los seres humanos, sí que “*es posible establecer una categoría legal especial para los robots... en el concepto ya existente de personalidad jurídica*”<sup>89</sup>. Es cierto que la personalidad jurídica no deja de ser un artificio, una ficción creada por el Derecho para dotar de derechos y obligaciones al actor de la misma. Por lo tanto, jurídicamente podría ser viable dotar de esa personalidad a los robots, ampliando esa ficción e incluyendo en ella a los robots.

Afirma en esta línea LACRUZ MANTECÓN que “*las bases para una personalidad robótica, sea esto lo que sea, no pueden basarse en la IA, sino en meros motivos de oportunidad y necesidad*”<sup>90</sup>. En cambio, sostiene ERCILLA que el elemento

88 Como ya hemos visto el Parlamento Europeo apuesta porque se denomine persona electrónica, otros se inclinan por denominarla robótica y, los menos, por el término ciberfísica.

89 Vid. GUNTHER, J., MUNCH, F., BECK, LOFFLER, S. y LABRUTO, R., “Issues of privacy and electronic... Op. cit., pág. 818

90 Vid. LACRUZ MANTECÓN, M.L.: “Potencialidades de los robots y capacidades de las personas”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018, pág. 77

básico que hay que tener en cuenta a la hora de determinar qué robots deben de tener personalidad jurídica es, precisamente, la autonomía. De este modo, basándose en la mencionada autonomía de los robots entendida esta como el hecho de no estar sometidos a la total voluntad humana, y a la capacidad de aprender del entorno a través de la inteligencia artificial, “*resulta así conveniente la creación de dicha personalidad jurídica por razones de pura organización de entes no sometidos a la total voluntad humana, sino consecuencia del mundo que les rodea*”<sup>91</sup>.

Tomaré, a la hora de realizar el análisis correspondiente, esta última postura, mayoritaria entre la doctrina que defienden la necesidad de dotar de personalidad jurídica no a todos los robots, sino tan solo a aquellos que gocen de cierta autonomía con respecto al ser humano a la hora de tomar decisiones.

La cuestión sobre la necesidad o no de dotar de personalidad jurídica a los robots no solo ha surgido en el ámbito del Derecho civil, sino que también lo ha hecho con fuerza en el campo del Derecho laboral y del Derecho tributario. La relativa al Derecho civil la estudiaré con profundidad a continuación, pero ya anticipo que se basa en la posibilidad de hacer a los robots sujetos de derechos y obligaciones para así poder formar parte del tráfico jurídico, llegando las propuestas doctrinales a hacerlos responsables de los daños que puedan provocar.

Como señalaba, en la doctrina laboral y tributaria se debate sobre la necesidad o no de establecer algún tipo de gravamen para el uso de los robots en el ámbito laboral. La discusión gira en torno a si los robots pudieran ser considerados trabajadores y si se les debiera gravar con algún tipo de impuesto. Tanto es así que algunos autores han llegado incluso a plantear propuestas sobre la inclusión o modificación de tipos impositivos concretos. Así, SEGURA ALASTRUÉ llega a preguntarse si un impuesto sobre los robots debe incluirse en “*el ámbito de la tributación sobre las personas jurídicas o se trasladaría al Impuesto sobre la Renta de las Personas Físicas, dado que sustituiría al gravamen de un trabajador*”<sup>92</sup>.

---

91 “*Así, aquellos que fueran capaces de aprender del entorno a través de la inteligencia artificial y de distinguirse de los demás de su misma versión, por las circunstancias en torno a las cuales ha descrito su existencia, precisarían –por su condición de seres autónomos relacionables con la sociedad– de un estatus jurídico distinto... la necesaria creación de un tertium genus de personalidad, a parte de la persona física y la persona jurídica, se hará presente en el momento disruptivo en que pueda afirmarse la individualidad de cada robot por las circunstancias en torno a las cuales se ha desarrollado su existencia, definiéndose como ente inteligentes y volentes.*” Cfr. ERCILLA GARCÍA, J.: “Aproximación a una Personalidad Jurídica Específica para los robots”, en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n°47, 2018, pág. 4

92 Cfr. SEGURA ALASTRUÉ, M: “Los robots en el Derecho financiero y tributario”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluwer, pág. 174

Igualmente, y en el ámbito laboral, hay una parte de la doctrina que defiende la necesidad de que las empresas que utilicen robots dotados de inteligencia artificial deban cotizar por ellos a la seguridad social<sup>93</sup>. Eso implicaría, con la redacción actual del artículo 7.2 del Real Decreto 2064/1995, de 22 de diciembre, por el que se aprueban el Reglamento General sobre la Cotización y Liquidación de otros derechos de la Seguridad Social, que debería dárseles el mismo tratamiento que a las personas físicas o jurídicas. Así, afirma el precepto que “*están sujetas a la obligación de cotizar a la Seguridad Social las personas físicas o jurídicas...*” GÓMEZ SALADO propone, para solventar este inconveniente, la creación de “*una personalidad para los robots*” a las que denomina personas robóticas o personas electrónicas y a los que se les atribuirían “*derechos y obligaciones*”<sup>94</sup>. En mi opinión, como seguidamente expondré, las obligaciones tributarias o laborales no las debería tener los robots, sino los propietarios de los mismos, por lo que se podría perfectamente recaudar, en caso de que ello fuere necesario, tanto en cotizaciones a la seguridad social como en impuestos por la utilización de los robots en actividades laborales sin necesidad de dotarlos de personalidad jurídica alguna<sup>95</sup>. Así, en lo referente a los gravámenes, se manifiesta HIDALGO PÉREZ que se muestra en su trabajo contrario al establecimiento de un impuesto por el uso de los robots, aunque afirma que existe un debate al respecto y que “*adquiere, de este modo, relevancia la idea de diseñar una imposición al factor que supuestamente sustituye al trabajador y, por ello, se apropia de su renta, la máquina o el robot*”<sup>96</sup>.

Por ello, no creo que dotarlos de personalidad sea la solución puesto que el problema que se plantea se podría salvar bien con la modificación del citado artículo 7.2, así como con la introducción de un posible gravamen destinado, no a los robots en sí mismos, sino a aquellas personas jurídicas o físicas que utilicen a estos como bienes de producción. Como posteriormente defenderé, los robots tendrían más encaje dentro de la clasificación de cosas, eso sí, con determinadas especificidades que hagan que la inclusión de los robots en el tráfico laboral y económico pueda generar más beneficios que perjuicios, que en el de personas.

Ya adentrándonos en el ámbito civil, autores como BARRIO ANDRÉS, defienden la necesidad o conveniencia de crear una nueva categoría, además de las tradicionales personalidades físicas y jurídicas reconocidas histó-

93 GÓMEZ SALADO, M.A.: “Robótica, empleo y seguridad social. La cotización de los robots para salvar el actual estado del bienestar”, en *Relaciones laborales y Derecho del empleo*, Vol. 6, °3, 2018, pág. 161

94 GÓMEZ SALADO, M.A.: “Robótica, empleo y seguridad social... Op. cit. pág. 165

95 Es cierto que existe un amplio debate sobre la materia, aunque ni si quiera los expertos se ponen de acuerdo a la hora de establecer si la imposición por el uso de robots es conveniente

96 Cfr. HIDALGO PÉREZ, A.: “Robots e impuestos”, en *ICE, Revista de Economía*, núm. 917, 2020, pág. 218

ricamente. De este modo, sostiene que los robots deben de ser considerados personas electrónicas en tanto en cuanto son capaces de tomar decisiones de manera autónoma e inteligente, que les permitiría relacionarse con personas<sup>97</sup>. Esa personalidad, en palabras de otros de los defensores de esta postura como es VALENTE, implicaría “*considerar a los robots como una persona de derecho que tiene ciertos derechos y obligaciones de carácter meramente instrumental para un interés económico específico de un ser humano*”<sup>98</sup>.

La base argumental, pues, de esta parte de la doctrina para defender la creación de un nuevo tipo de personalidad, se encuentra en la idea de que los robots son seres autónomos dotados de cierta inteligencia, y con capacidad para relacionarse en sociedad, por lo que deben de poder ser sujetos de derechos y obligaciones. Trataré a continuación de demostrar que ello no es necesario y que, de llevarse a cabo, conllevaría más inconvenientes y riesgos que ventajas.

### 3.2. El Robot como cosa

Ya para Gayo, todo el derecho se dividía en personas, cosas y acciones que habían sido objeto de *summae divisiones* y que cubrían todos los supuestos<sup>99</sup>. Así, sin salirnos del esquema tradicional, los robots se seguirían encontrando entre las cosas, pero con un estatuto jurídico que los distinguiese, por sus características especiales, del resto de bienes y animales.

Parece evidente que aquellos elementos que cuenten con inteligencia artificial, con el marco jurídico actual, no se podrán considerar personas físicas puesto que el artículo 30 del Código civil señala que “*La personalidad se adquiere en el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno.*” Tampoco podría incluirse entre las personas jurídicas recogidas en el artículo 35 del Código civil, que se refiere a las corporaciones, asociaciones y fundaciones de interés público, por lo que algunos autores han propuesto la creación de una nueva categoría jurídica, la persona electrónica, que permita otorgar derechos y obligaciones coincida con las características que presenta un robot<sup>100</sup>. Así pues, hemos de descartar, sin duda alguna, la posibilidad de que los robots puedan ser consideradas personas físicas, por mucho que pueda avanzar esta técnica dotando de inteligencia y autonomía a los mismos.

---

97 Vid. Por todos, BARRIO ANDRÉS, M. *Derecho de los robots*, Ed. Wolters Kluwer, 2019

98 VALENTE, L.A.: “La persona electrónica”, en *Anales de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de la Plata*, Vol. 16, núm. 49, 2019, pág. 13

99 WEGMANN STOCKEBRAND, A.: “Sobre la noción de contrato en las instituciones de Gayo”, en *Revista de Derecho Privado*, n°34, 2018, pág.27

100 HERNÁNDEZ GIMENEZ, M.: “Inteligencia Artificial y Derecho Penal”, en *Actualidad jurídica iberoamericana*, n° 10 bis, 2019, pág. 803

Es cierto que la Resolución del Parlamento Europeo sobre normas de Derecho Civil sobre robótica apuesta por “*crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas...*” Ya en el pionero informe Robolaw, se debatía esta posibilidad, analizando si los robots podrían cumplir los requisitos básicos para otorgarles personalidad jurídica, de forma análoga a como ya se hace con las personas jurídicas<sup>101</sup>. Pero, como ya he anticipado y ahora defenderé con mayor detenimiento, el dotar a los robots de personalidad jurídica no me parece una solución adecuada porque, entre otras razones, las personas, tanto jurídicas como físicas, tienen, al menos, dos características comunes; En primer lugar, ambas pueden ser titulares de derechos y de obligaciones, algo que no sucede con los robots. Y, en segundo, tras las dos figuras mencionadas está siempre detrás el ser humano. De una forma, o de otra. Individualmente o de forma colectiva.

### 3.2.1. *Imposibilidad de los robots para ser titulares de derechos y obligaciones*

Respecto a la primera, el hecho de que los robots pudiesen ser titulares de derechos y obligaciones, hemos de descartar la posibilidad de que lo pudiesen ser. Lo serán, en cualquier caso, los propietarios de estos. Es cierto que algunos autores, como hemos visto, han sostenido que sí podrían serlo. De este modo, SHRAFIAN defiende que “*el primer derecho de un robot sería el derecho a estar libre del dolor y el sufrimiento*”, como muestra del Derecho a la integridad física<sup>102</sup>. No comparto este argumento. Los robots no sufren, al menos no ahora, y tampoco sienten dolor alguno como sí lo hace el ser humano. Me costaría comprender que en algún momento del futuro pudiese suceder. Es más, llegado el caso en el que se pudiese realizar un software que permitiese a los robots sentir algo parecido al sufrimiento humano, cosa que dudo, serían las normas éticas las que debería prohibir esa posibilidad. En términos similares se ha manifestado LEAN LAU, que rechaza de pleno otorgar personalidad jurídica a los robots, a pesar de que cuenten con inteligencia artificial, principalmente porque estos no tienen ni conciencia ni intencionalidad<sup>103</sup>. Pueden tener autonomía, pero eso no les dota, ni lo hará en un futuro, de humanidad.

En definitiva, no alcanzo a ver los derechos de los que gozaría un robot, puesto que no les serían aplicables los derechos reconocidos a los trabajadores, personas físicas, como las vacaciones, el descanso o el pago de un salario. ¿Acaso se propone que los robots dejen de producir durante 16 horas al día para que tengan una jornada laboral homologable a la de los seres

101 Vid. PALMERINI, E. (2014), *The RoboLaw Project...* Op. cit. pág. 19

102 Vid. SHRAFIAN, H. “AIonAI: A Humanitarian Law of Artificial Intelligence and Robotics.”, en *Science and Engineering Ethics*, 2015, pág. 32

103 Vid. LEAN LAU, P: “The Extension of Legal Personhood in Artificial Intelligence”, en *Revista de Bioética y Derecho*, n° 46, pág 56

humanos? Es evidente el objetivo de una jornada laboral limitada para las personas físicas, pero ¿qué sentido tendría limitar el periodo laboral de los robots?

Más aún deberíamos descartar que a los robots se les reconociesen derechos similares a los fundamentales de los seres humanos. Esto último nos podría llevar a un absurdo similar al que se produjo en el Estado de Nueva York en el año 2015, en el que una juez concedió a dos chimpancés que estaban siendo utilizados para experimentación biomédica un hábeas corpus, lo que nos lleva a concluir que el Tribunal ha determinado implícitamente que fueron tratados como personas. Me cuesta imaginar, evidentemente, que eso mismo pudiese suceder con los robots<sup>104</sup>.

Al igual que tampoco podrían ser titulares del derecho de propiedad o disponer de un patrimonio, aunque haya quien sostenga que esto es necesario, como ahora veremos, para resolver la cuestión relativa a la responsabilidad civil. Lo mismo sucedería con las personas jurídicas, que pueden ganar dinero, ser titulares de bienes, mientras que los robots no. Pueden hacerlo para sus propietarios, pero no para sí mismos.

Afirma SOLAIMAN, refiriéndose a un trabajo de SALMOND, que la capacidad de disfrutar de derechos y cumplir obligaciones es exclusiva de las personas físicas o jurídicas, por lo que, a la inversa, conferir personalidad jurídica está intrínsecamente relacionado con la concesión de derechos jurídicos y la imposición de obligaciones jurídicas<sup>105</sup>. Un argumento similar al expuesto fue ya utilizado en el mencionado informe *Robolaw* para negar la posibilidad de dotar a los robots de personalidad, sea cual fuere la denominación que se le diese a esta, porque “*no se podrán reconocer derechos a los robots*”<sup>106</sup>.

Distinto es que, como defiende ERCILLA, los robots puedan llegar a realizar muchos de los negocios jurídicos que podría realizar una persona física o jurídica, “*pero no para sí, sino para su dueño*”<sup>107</sup>. Pero esta circunstancia no es

---

104 SCHNEIDER, K. (2020). Judge Recognizes Two Chimpanzees as Legal Persons, Grants them Writ of Habeas Corpus (Blog). Accesible en <https://www.nonhumanrights.org/blog/judge-recognizes-two-chimpanzees-as-legal-persons-grants-them-writ-of-habeas-corpus/>

105 “*En cambio, si nos atenemos a nuestro requisito de ser titular de derechos y deberes, es improbable que los robots cumplan este requisito esencial, dado que son productos fabricados por el hombre con un autocontrol limitado, tal como se ha programado hasta la fecha, en particular los utilizados en los sectores industrial y social*” Cfr. SOLAIMAN, S.M.: “Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy”, en *Artif Intell Law*, 2017, pág.158

106 Vid. PALMERINI, E. (2014), *The RoboLaw Project...* Op. cit. pág. 190

107 Realiza este autor un paralelismo entre la posible personalidad de los robots y la de los esclavos de la antigua Roma. En este sentido afirma que “*al igual que los esclavos en la antigua Roma, carecería el robot de ius connubii, esto es, de capacidad jurídica personal para contraer matrimonio, extremo este al que ya hace referencia el Parlamento Europeo en su recomendaciones, al señalar como principio general, evitar los vínculos emocionales con los robots. Así mismo también carecería el robot, a semejanza del esclavo, de ius commercii, esto es, de capacidad jurídica patrimonial, dado que si bien podría*

novedosa en el Derecho. Entiendo que, en ese caso, la voluntad de llevar a cabo el negocio jurídico, así como las instrucciones para el acuerdo de este, no partirían del robot, sino de su dueño. Incluso poniéndonos en que esta circunstancia fuese posible, convertiría a los robots en un simple instrumento, sin posibilidad de ser titular de derecho u obligación alguna. Salvando las distancias, el papel de los robots que propone este autor no se alejaría del que realiza cualquier máquina expendedora que pertenece a un titular, ya sea persona física o jurídica, y que realiza un negocio jurídico, compraventa, en nombre de este. Efectivamente, la máquina no adquirirá el derecho de cobro, puesto que este derecho seguirá siendo del titular de la máquina, ni tendrá la obligación de entregar el objeto por el que paga el consumidor, porque la obligación seguirá siendo, nuevamente, del titular de la máquina. Es por ello por lo que el mero hecho de ser un instrumento en un negocio jurídico no tiene por qué conllevar la necesidad de dotar de personalidad alguna para los robots, igual que no lo tienen las máquinas expendedoras, más o menos avanzadas tecnológicamente hablando. Imaginemos incluso que esa máquina expendedora estuviese dotada de inteligencia artificial y, en base a unos algoritmos previamente introducidos y a los datos que va recabando de la demanda del producto en cada momento, es la propia máquina la que va fijando el precio del producto. Cumpliría con los requisitos que sostienen una parte de la doctrina para dotar de personalidad jurídica a la máquina, como la de tener cierto grado de autonomía.

En este sentido, hay autores que han mantenido la posibilidad de que los robots, en casos como el último de los citados, aunque no se les dotase de personalidad, sí que se les pudiese atribuir una capacidad jurídica limitada<sup>108</sup>. Pero ello, en mi opinión, tampoco justificaría la necesidad de dotar ni de personalidad jurídica ni de capacidad de obrar a la máquina, aunque actuase en cierta medida de manera autónoma, puesto que podría desarrollar esa actividad en las mismas condiciones en las que las viene prestando en la actualidad. La capacidad es de la persona que realiza el negocio jurídico, el robot tan solo es un mero instrumento a través del cual esta se manifiesta esta. El contratante, como parte del contrato, asume desde el inicio las condiciones en las que se celebrará, y debería contar con el conocimiento de los algoritmos que ha-

---

*actuar en el tráfico jurídico, al tener capacidad de obrar, siempre lo haría en nombre y representación de su propietario. De tal modo que todo lo que adquiriese, pasaría al patrimonio del dueño.*” Cfr. ERCILLA GARCÍA, J.: “Aproximación a una Personalidad... Op. cit., pág. 6

108 De este modo, algunos autores sostienen que “*otro enfoque podría consistir en considerar a esos agentes de programas informáticos como objetos con capacidad jurídica limitada, de conformidad con la ley de la esclavitud en el derecho civil. En el derecho civil romano, los esclavos no tenían capacidad para tener derechos y obligaciones mientras actuaban en su propio nombre. No tenían derecho legal a celebrar contratos en su propio nombre, pero podían celebrar contratos como agentes de su amo*”, Cfr. GUNTHER, J., MUNCH, F., BECK, LOFFLER, S. y LABRUTO, R., “Issues of privacy and electronic personhood in robotics. Proceedings”, *IEEE International Workshop on Robot and Human Interactive Communication*, 2012, pág. 817

rán que el contrato se perfeccione de una u otra manera. Asume que el robot, a través de las instrucciones que se le hayan dado con carácter previo, será el que determine, por ejemplo, el precio final de la compra. Pero el hecho de que el contratante no conozca el resultado final, puesto que dependerá del robot, no es una novedad en nuestro Derecho que genere la necesidad de dotar de personalidad jurídica o capacidad a este. Bien al contrario, esta circunstancia también se da, entre otros casos, en los contratos aleatorios, en los que hay una indeterminación inicial del resultado final, que dependerá de alguna circunstancia desconocida por las partes.

Lo mismo sucede con las aerolíneas. Los billetes de avión van modificando continuamente el precio a través de los algoritmos y datos con los que cuenta el software, como número de plazas restantes, la mayor o menor demanda o búsqueda del destino, la previsión meteorológica u otros muchos. Sea como fuere, la contratación se realiza directamente online, sin la participación de la persona jurídica, lo que no implica que haya que dotar de personalidad al software, que ya viene participando de manera activa en el tráfico jurídico sin necesidad de esta.

Comparto el argumento de PAGALLO cuando afirma que se “*pueden abordar adecuadamente los desafíos de la condición de los robots con inteligencia artificial en los contratos y el derecho comercial, sin abarcar ninguna forma de corporación y por lo tanto, cualquier tipo de personalidad jurídica de Robots de IA*”<sup>109</sup>. Y esto no solo lo demuestra el hecho de que desde hace décadas los robots vengán participando de una forma u otra en el tráfico jurídico sin la necesidad de atribuirles de personalidad jurídica alguna, sino que su estatus legal actual de cosas, ha sido eficaz.

Como ya avancé al inicio del presente epígrafe, otro de los argumentos que hacen que me incline por negar la posibilidad de otorgar personalidad a los robots es el hecho de que detrás de estos haya siempre, en cualquier caso, una persona. Una persona que puede ser física o jurídica, pero que hace innecesario el otorgamiento de personalidad a los robots. De este modo, detrás de cualquier persona jurídica hay una gestión de esta por parte de personas físicas. Las personas jurídicas, en cualquier caso, siempre están compuestas de un modo u otro por seres humanos<sup>110</sup>. Como previamente señalaba, será siempre el ser humano, bien individualmente considerado

---

109 Este autor sostiene que “*en cuanto a la personalidad jurídica de los robots de IA, el estado actual de la técnica ha sugerido que ninguno de los actuales robots cumplen los requisitos que normalmente se asocian con la concesión a alguien, o a algo, de tal estatus legal.*” Cfr. PAGALLO, U.: “Vital, Sophia, and Co.—The Quest for the Legal Personhood of Robots”, en *Information* n.º 9

110 Esta misma argumentación fue utilizada por un grupo internacional de expertos en una misiva que remitieron a la Comisión Europea solicitando que no se dote a los robots de personalidad alguna. Concretamente sostenían los siguientes argumentos:

1) “*El estatuto jurídico de un robot no puede derivarse del modelo de Persona Natural, ya que el robot tendría entonces derechos humanos, como el derecho a la dignidad, el derecho a su integridad, el derecho a la remuneración o el derecho a la ciudadanía, con lo que se enfrentaría directamente a los derechos*

o socialmente unido, el elemento esencial de la persona física, en el primer caso, y de la persona jurídica, en el segundo. Toda la teoría clásica sobre la personalidad jurídica está ligada a agrupación humana.

Ese es el motivo por el que a las personas jurídicas pueden tener intenciones y objetivos de los que responderían, porque son formadas por una colectividad de personas físicas. Los robots, precisamente porque carecen de esa estructura de la que forma parte el ser humano, es imposible que tenga esas intenciones y esos objetivos. Es cierto que algunos autores han sostenido la necesidad de introducir cambios en éste área, unos cambios que pasarían por desligar la dependencia de las personas jurídicas del ser humano<sup>111</sup>. En cambio, en los robots, que pueden llegar a ser autónomos, pueden no depender de una persona física como sí lo hacen las personas jurídicas. Por lo tanto, ese nuevo artificio rebasaría con mucho el ideado durante todos estos siglos como arquitectura fundamental de nuestro Derecho civil.

Otros argumentan la posibilidad de dotar de personalidad jurídica a los robots en la existencia de voluntad. Así, las personas físicas contarían con voluntad propia, las personas jurídicas, con voluntad común derivada de voluntades aisladas y, por último, la de los robots, dotados de una voluntad surgida de procesos algorítmicos.<sup>112</sup> Aunque esa voluntad realmente no es de los robots, es de aquellos que los programan.

### 3.2.2. *La personalidad de los robots como medio para hacer frente a la responsabilidad civil*

Como decía anteriormente, el segundo de los motivos por el que no creo que sea razonable ni conveniente dotar a los robots de personalidad jurídica es el relativo a su posible responsabilidad civil. De este modo, algunos

---

*humanos. Esto estaría en contradicción con la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales.*

2) *La condición jurídica de un robot no puede derivarse del modelo de Entidad Jurídica, ya que implica la existencia de personas humanas detrás de la persona jurídica para representarla y dirigirla. Y este no es el caso de un robot.*

3) *El estatus legal de un robot no puede derivar del modelo de Fiducie o Treuhand anglosajón en Alemania. De hecho, este régimen es extremadamente complejo, requiere competencias muy especializadas y no resolvería la cuestión de la responsabilidad. Y lo que es más importante, seguiría implicando la existencia de un ser humano como último recurso -el fideicomisario o fiduciario- responsable de la gestión del robot concedido con un Trust o un Fiducie.”*

Vid. Open Letter to the European Commission Artificial Intelligence and Robots, 2018. Accesible en <http://www.robotics-openletter.eu/>

111 Sostiene DYSCHKANT que hay que “divorciar la definición de personalidad jurídica centrada en las capacidades de la definición de humanidad basada en las especies”. Cfr. DYSCHKANT, A.: “Legal Personhood: How We Are Getting It Wrong”, en *University of Illinois Law Review*, n° 36, 2015, pág. 76

112 ERCILLA GARCÍA, J.: “Aproximación a una Personalidad Jurídica Específica...”, Op. cit., pág. 3

autores han argumentado la idea de que los robots, al contrario de lo que defiendo yo, puedan ser titulares de un patrimonio en base a la idea de que ésta podría ser una solución a la problemática de la responsabilidad civil de aquellos. Así, ese patrimonio sería usado para responder de los daños que los robots pudiesen llegar a causar. Aunque más tarde me detendré para analizar ampliamente esta circunstancia el capítulo relativo a la responsabilidad civil, haré una breve referencia llegado a este punto.

No son pocos los autores que defienden el hecho de dotar de personalidad a un robot podría llegar a significar que este fuese directamente el responsable de los daños que llegue a causar<sup>113</sup>. Algunos autores han llegado a afirmar que el motivo por el que se pretende dotar de personalidad a los robots es para que sean responsables de los daños que causasen, eximiendo así de cualquier tipo de responsabilidad a los fabricantes de estos<sup>114</sup>.

ERCILLA, apuesta por esta vía a través de una curiosa e interesante comparación entre el patrimonio de los robots y el *peculio* de los siervos de la antigua Roma, que eran todos los bienes que el *dominus* atribuía voluntariamente a aquel. Así, propone que los robots acumulasen un patrimonio a través de un porcentaje de lo que produjesen. Una parte iría destinada al patrimonio del dueño del robot, y otro al robot mismo<sup>115</sup>. Mi postura es contraria a esta idea, puesto que la propuesta realizada dejaría de tener sentido con la simple exigencia de la suscripción de un seguro de responsabilidad civil obligatorio al dueño del robot, propuesta que se incluye en las recomendaciones que el Parlamento Europeo ha enviado a la Comisión Europea para que sea tenida en cuenta a la hora de actualizar la legislación comunitaria en esta materia. Más tarde volveré sobre esta cuestión en el capítulo dedicado a la responsabilidad civil.

Este hecho, en mi opinión, es una línea que no podemos rebasar. No podemos permitir que los robots asuman la responsabilidad de los daños que ellos causen abriendo la puerta a la posible exención de esa responsabilidad a los operadores o fabricantes de los mismos. Se ha dicho, acertadamente, que, si esta circunstancia se llegase a permitir, podríamos correr “*el riesgo de que la personalidad electrónica protegiere a algunos actores*”

---

113 Vid. PALMIERI, E., “Robótica y derecho: sugerencias, confluencias, evoluciones ... Op. cit., pág. 78

114 NAVEJANS y SHARKEY han mantenido esta postura en distintas ocasiones. Recogido en “Europe divided over robot ‘personhood’”, *Politico*, 2018. Accesible en <https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood/>

115 El autor pone el ejemplo de cómo podría llevarse a cabo este sistema con un coche autónomo: “*En consecuencia, si partimos del ejemplo antedicho, vehículos autónomos particulares que sirven de taxi durante los tiempos de desuso, el patrimonio que el vehículo fuera conformando por su actuación comercial, podría ser gestionado por la inteligencia artificial del mismo, como si del peculio romano se tratara, pudiendo operar en distintos mercados bursátiles o de criptoactivos, obteniendo un rendimiento a dicho dinero*” Cfr. ERCILLA GARCÍA, J.: “Aproximación a una Personalidad... Op. cit., pág. 6

*humanos de la responsabilidad de violar los derechos de otros actores, particularmente humanos*<sup>116</sup>.

Este es, sin lugar a dudas, otro de los límites que impiden que los robots puedan llegar a tener personalidad jurídica alguna. Y no se trata de un hecho novedoso en nuestra historia -el de usar la atribución de personalidad jurídica para eximir de responsabilidad a las personas físicas- puesto que, como ya decía COSSIO, en ocasiones se recurre al uso abusivo de la personalidad jurídica “*con la intención de limitar la responsabilidad individual*”<sup>117</sup>.

Aunque es cierto que el hecho de que se les reconozca algún tipo de personalidad a los robots no tiene por qué llevar aparejada de forma directa la responsabilidad de los mismos, es evidente que se trataría de una posibilidad. En ese caso, no quedaría otra salida que aplicar lo previsto en la responsabilidad civil extracontractual, al igual que puede llegar a suceder con la responsabilidad de los empresarios por los daños causados por sus empleados recogido en el artículo 1.903 del Código civil, y se les haga responsables de los daños causados por sus robots/productos a los propietarios o fabricantes de los mismos.

No parece lógico querer hacer responsables a los robots, que, como hemos señalado, carecen de derechos y, por lo tanto, de legitimidad procesal y patrimonio alguno con el que responder ante los daños causados, por mucho que, como señalaremos más adelante, algunos pretendan crear un patrimonio de los robots. En este último sentido afirma GÓMEZ-RIESCO que “*incluso en el caso de que se les reconociera tal personalidad, parece difícil que se pueda actuar contra el propio robot para indemnizar los daños, pues el robot carecería de propiedades a su nombre, salvo que estimemos que responde con su propio valor económico y como activo que pueda ser incautado, embargado o enajenado para que, con su precio, se pueda resarcir la persona que ha sufrido el daño, todo ello sin perjuicio, además, de los problemas procesales para reconocer legitimación pasiva a los robots en un procedimiento judicial*”<sup>118</sup>.

Otro de los riesgos que se corre con la propuesta de dotar de personalidad a los robots para que estos asuman directamente la responsabilidad de sus actos, es desnaturalizar uno de los objetivos de esta, que no es otra que el de disuadir a las personas de cometer daños. Es cierto que, en el ámbito civil, el principal objeto de la responsabilidad es el de resarcir el daño causado, pero no podemos olvidar la existencia de esa segunda vertiente, espe-

116 Vid. Bryson, J.J.; Diamantis, M.E.; Grant, T.D. “Of, for, and by the People: The Legal Lacuna of Synthetic Persons.” *Artif Intell Law* 2017, n° 23, pág. 287

117 COSSIO CORRAL, A.: “Hacia un nuevo concepto de la persona jurídica... Op. cit., pág. 645

118 Cfr. GÓMEZ-RIESCO TABERNERO DE PAZ, J.: “Los robots y la responsabilidad civil extracontractual”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluwer, pág. 111

cialmente en el ámbito penal, la disuasión como medio para anticiparse a la producción del daño<sup>119</sup>.

### 3.2.3. *Un nuevo estatus como cosa*

Las cosas no tienen ni derechos ni obligaciones, ni pueden ser responsables por los daños que produzcan. Son, en cualquier caso, tan solo objetos de esos derechos que tienen las personas físicas y jurídicas. Lo mismo sucede en el ámbito de la responsabilidad civil. Las personas, tanto físicas como jurídicas, responden civilmente de los daños causados por ellos o incluso por terceras personas. Así pues, todo lo más sería la creación de un estatus especial para los robots, dentro de las cosas, sin necesidad de dotarlos de personalidad.

Comparto la vehemente postura de ROGEL VIDE en este tema cuando sostiene que “*los robots son máquinas, cosas, todo lo singulares que se quiera; mas no pueden ser personas, sujetos de derechos, y sí solo objetos de los derechos dichos, singularmente el de propiedad y cualesquiera otros reales*”<sup>120</sup>.

No es descabellada la idea de crear un nuevo estatuto jurídico, que los diferencia tanto de las cosas como de las personas. Algo similar ha sucedido en el Código civil francés en el que los animales, aun siendo bienes, no se les equipara a las cosas, sino que son considerados como “*seres vivos dotados de sensibilidad*”<sup>121</sup>. En nuestro País se aprobó una reforma en el mismo sentido para modificar el Libro segundo del Código civil que ha pasado a como *De los animales, de los bienes, de la propiedad y de sus modificaciones*.<sup>122</sup> Incluso hay quién ha propuesto llegar más allá, modificando el concepto de persona jurídica, incluyendo una nueva categoría que incluya a los animales, con la intención de aumentar la protección legal de estos, postura esta exagerada según mi opinión<sup>123</sup>.

Algunos autores, al descartar la posibilidad de que los robots puedan ser considerados como personas jurídicas, han sostenido que podrían asemejarse más a los animales, aunque uno sea un producto creado por el hombre y el otro un ser vivo. Tanto es así que “*ambos se consideran como propiedad y, por lo*

---

119 Para un análisis de la disuasión como fundamento de la responsabilidad civil es interesante el trabajo de TENA. Vid. TENA R.: “Hacia un salto evolutivo en el Derecho civil: de la justicia conmutativa a la disuasión”, en *El Notario*, n°90, 2020

120 Vid. ROGEL VIDE, C.: “Robots y personas”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018, págs. 16 y 17

121 Art. 515-14 del Código civil francés: “*Los animales son seres vivos dotados de sensibilidad. Bajo reserva de leyes que los protegen, los animales están sujetos al régimen de los bienes*”

122 Cfr. Ley 17/2021, de 15 de diciembre, de modificación del Código Civil, la Ley Hipotecaria y la Ley de Enjuiciamiento Civil, sobre el régimen jurídico de los animales. Boletín Oficial del Estado núm. 300, de 16 de diciembre de 2021.

123 KURKI, A.J. y PIETRZYKOWSKI, T.: *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Ed. Springer, 2017

*tanto, son meros objetos de la ley, en lugar de sujetos*<sup>124</sup>. En este mismo sentido se ha posicionado SANTOS GONZÁLEZ que considera inadecuado el uso del término persona para identificar a un robot, ya que los robots no pueden englobarse dentro éste, puesto que “*el robot es tecnología independiente de la persona*”<sup>125</sup>.

De este modo, son muchos los autores que defienden que para que las empresas o personas dueñas de robots tuviesen que cotizar por él no necesariamente implicaría que se les haya de dotar de algún tipo de personalidad, aunque sí que debe poder diferenciarse de manera clara qué robots implicarían esa nueva obligación tributaria. SÁNCHEZ-URÁN y GRAU llegan a la conclusión de que, aunque el Derecho del trabajo haya de reflexionar sobre la posibilidad de que los robots puedan tener un estatuto laboral, no debería incluirse a estos dentro de la categoría de personas, aunque sí “*podría avanzarse en relación con los robots interactivos en su consideración de tercero que acompaña al humano en la ejecución de su trabajo*”<sup>126</sup>. La denominación, aunque siempre es relevante, no es lo sustancial, sino las atribuciones que se darían a ese robot como sujeto, entiendo que únicamente de obligaciones, que no de derechos. Esa sería la principal diferencia con las personas, tanto jurídicas como físicas.

En definitiva, no es que jurídicamente no se pueda dotar de personalidad a los robots, que se puede, sino que no considero que aporte solución alguna, más bien al contrario. A lo largo de este capítulo he mantenido esta postura basándome en argumentos, tanto teóricos como pragmáticos. Los teóricos, fundamentalmente, se basan en dos premisas: Primero, las personas, ya sean físicas o jurídicas, son titulares de derechos y de obligaciones, los robots no. La segunda, detrás de cualquier persona, física o jurídica, siempre es el ser humano el que toma las decisiones -personalmente o de manera interpuesta-, cosa que no sucedería en el caso de los robots autónomos que fuesen capaz de tomar decisiones prescindiendo de los humanos.

Los pragmáticos se basan en el hecho de que dotar a los robots de personalidad no solventaría los principales problemas que plantean, bien al con-

124 Vid. SOLAIMAN, S.M.: “Legal personality of robots...”, Op. cit., pág.176

125 Cfr. SANTOS GONZÁLEZ, M.J.: “Regulación legal de la robótica y la inteligencia artificial: Retos de futuro... Op. cit. pág. 43

126 “*El Derecho del Trabajo permite posicionarse críticamente sobre la personalidad robótica o sobre los ECNP, es decir sobre el reconocimiento en el plano jurídico de una nueva categoría de sujetos o entes capaces, más aún cuando se trata de definir una relación, como la laboral, de contenido patrimonial-personal de intercambio permanente y estable y, sobre todo, voluntario; voluntariedad, consciencia, que no alcanza a los robots aunque estén provistos de sistemas de IA.*” SÁNCHEZ-URAN AZAÑA, M.Y., y GRAU RUIZ, M.A.: *El impacto de la robótica, en especial la robótica inclusiva, en el trabajo: Aspectos jurídico-laborales y fiscales*. Ponencia presentada al Congreso Internacional sobre INNOVACIÓN TECNOLÓGICA Y FUTURO DEL TRABAJO, Santiago de Compostela, 5 y 6 de abril de 2018, pág. 19 y 20

trario. Por un lado, quizá el más relevante, el hecho de que respondiesen civilmente los propios robots por los daños causados tan solo abriría la puerta a la posible exención, total o parcial, del fabricante o del dueño de este. El supuesto beneficio de que asumiesen el pago de las indemnizaciones por daños y perjuicios a través de un patrimonio del que serían titulares, dotado por parte de los beneficios que generen, no deja de ser similar a la existencia de un seguro obligatorio de responsabilidad civil. Otro problema añadido sería el de la falta de legitimidad procesal, que abocaría a la imposibilidad de demandar única y exclusivamente al robot. Tampoco resolverían los problemas relacionados con el ámbito fiscal o laboral. Existen, en definitiva, otras fórmulas para poder solventar todos estos retos, que no pasan por el dotar de personalidad jurídica a estos. Todo ello se podría resumir, como señalaban un grupo de autores norteamericanos, en que “*sería moralmente innecesaria y jurídicamente problemática*”<sup>127</sup>.

Echo en falta que el sector doctrinal que apoya la necesidad de crear un nuevo tipo de personalidad para los robots exponga de forma clara y detallada qué problemas en el ámbito jurídico podría solventar la atribución de personalidad jurídica a estos. No basta con dotar de personalidad un ente, sino que hay que dotar de contenido esa personalidad. Las principales soluciones que algunos creen que aportaría esta propuesta, se limitan a la atribución directa de responsabilidad, sobre la que ya he manifestado mi parecer contrario, la de contar con un patrimonio propio y poder ser considerado personal laboral y así poder ser gravado con los correspondientes impuestos. Ninguna de estas propuestas, reitero, solucionan la problemática que plantean los robots. El de la responsabilidad, porque abre la puerta a la exención de la misma por parte de las personas físicas que realmente tendrían que responder, que como más tarde veremos girarán en torno al fabricante del robot, al creador del software y al propietario del mismo. Como ya he dicho, esa alternativa, que busca garantizar una parte de la indemnización que debería recibir aquel que sufra el daño, es fácilmente salvable con un instrumento ya habitual, la constitución de un seguro de responsabilidad civil obligatorio. Tampoco aporta mayor novedad en el ámbito laboral o fiscal, puesto que existirían alternativas en ambos campos que permitirían llegar al mismo fin, poder establecer, en su caso, cotizaciones sociales e impuestos por el uso de los robots, generalmente a quien se beneficie por la labor que lleven a cabo.

---

127 BRYSON, J. J., DIAMANTIS, M.E. y GRANT, T.D.: “Of, for, and by the people: the legal lacuna of synthetic persons”, en *Artif Intell Law*, 2017, pág. 1



# CAPÍTULO III

## LA INTELIGENCIA ARTIFICIAL Y LA NECESARIA PROTECCIÓN DE LA PRIVACIDAD

### 1. CONCEPTO DEL DERECHO A LA PROTECCIÓN DE DATOS

La inteligencia artificial, como ya hemos señalado, se caracteriza por ser capaz de tomar decisiones o proponerlas tras un tratamiento masivo de datos que, en muchos casos, pueden llegar a ser personales. La inteligencia artificial, por lo tanto, no tendría sentido alguno, ni utilidad, si no pudiese disponer de datos que le permitan analizarlos y aprovecharlos para, precisamente, tomar esas decisiones. Como afirma FERNÁNDEZ HERNÁNDEZ, “*la disponibilidad de datos es esencial para el desarrollo de unos sistemas de inteligencia artificial que están evolucionando rápidamente de la capacidad de reconocimiento de patrones y la generación de conocimientos al desarrollo de técnicas sofisticadas de predicción*”<sup>128</sup>. Ese uso masivo de datos puede, en ocasiones, afectar a datos de carácter personal, por lo que las autoridades públicas deben de establecer, a través de la legislación relativa a la protección de datos, medidas que protejan la privacidad de los ciudadanos.

Es por ello por lo que, aun no siendo mi intención realizar un estudio amplio sobre la protección de datos en sí misma, sí que se hace necesario, antes de estudiar las implicaciones principales que conlleva la aplicación de la inteligencia artificial en la protección de datos de carácter personal, realizar una breve introducción sobre la temática. Así, de manera somera y general, realizaré un breve análisis de la protección de datos, especialmente sobre el alcance del derecho, así como el concepto de dato personal, el tratamiento de los mismos y el consentimiento, antes de centrarme en la influencia que ésta tiene sobre la inteligencia artificial<sup>129</sup>.

---

128 FERNÁNDEZ HERNÁNDEZ, C.: “La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución”, en *Derecho digital e innovación*, nº5, 2020, pág. 1

129 Para ampliar sobre esta materia, APARICIO SALOM, J. y VIDAL LASO, M.: *Estudio sobre la protección de datos*, Ed. Aranzadi, 2019; BERROCAL LANZAROT, I.: *Estudio jurídico-crítico*

Una de las principales preocupaciones de la Unión Europea en materia de Inteligencia Artificial es asegurarse de que ésta actúa con respeto absoluto a los Derechos fundamentales. No se trata de que la protección de datos se convierta en un freno al desarrollo de la inteligencia artificial, sino que este se lleve a cabo con total respeto a los mismos. En palabras de MARTÍNEZ MARTÍNEZ, hemos de “asegurar un desarrollo de la tecnología que tenga en cuenta los derechos fundamentales no solo como límite, sino también como objetivo”<sup>130</sup>. Dicho de otro modo, el desarrollo de la inteligencia artificial tiene que ser, en cualquier caso, con pleno respeto a la protección de datos de carácter personal, lo que pasa por establecer, desde el diseño mismo de las aplicaciones con inteligencia artificial, una política respetuosa y compatible con la privacidad.

Esto mismo ha sido exigido por las autoridades públicas europeas. De este modo, como se recoge en el ya mencionado informe de la Comisión Europea sobre inteligencia artificial, uno de los aspectos legales a los que pide prestar mayor atención es el relativo a la protección de datos de carácter personal, pues hace referencia a un derecho fundamental, además de a la responsabilidad civil que trataremos con profundidad más adelante<sup>131</sup>.

El origen del Derecho a la protección de datos en Europa se remonta al Convenio de Roma para la protección de los derechos humanos y de las libertades fundamentales de 1950, en cuyo artículo 8 se reconoció el mencionado derecho como un derecho fundamental<sup>132</sup>. Si bien es cierto que la redacción se podría asemejar más al Derecho a la intimidad que al de protección de datos propiamente dicho, el desarrollo europeo de este último Derecho tiene en el mencionado Convenio su origen.<sup>133</sup> Así mismo, en el ámbito internacional, el Convenio 108 del Consejo de Europa<sup>134</sup> para la protección de las personas con respecto al tratamiento automatizado de datos

---

sobre la Ley orgánica 3/2018, de 5 de diciembre de 2018 de protección de datos personales y garantía de los derechos digitales, Ed. Reus, 2019; REBOLLO DELGADO, L.: *Protección de datos personales*, Ed. Dykinson, 2018

130 MARTÍNEZ MARTÍNEZ, R.: “Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo”, en *Revista Catalana de Dret Públic*, núm. 58, 2019, pág. 73

131 Op. cit. Comisión Europea (2018), *Inteligencia artificial...*, págs. 63 y ss.

132 En este trabajo me he centrado en el estudio de la protección de datos en Europa, aunque hay otras legislaciones igualmente interesantes. Para comparar nuestra legislación con la de Estados Unidos se puede consultar el breve pero interesante trabajo de SOBRINO GARCÍA. Vid. SOBRINO GARCÍA, I.: “Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos”, en *Revista de Derecho UNED*, núm. 25, 2019, págs.. 687-713

133 El artículo 8 del Convenio de Roma para la protección de los derechos humanos y de las libertades fundamentales de 1950 establece literalmente que “*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*”

134 Para un estudio más pormenorizado del Protocolo, Vid. PAVÓN PÉREZ, J.A.: “La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio

de carácter personal de 28 de enero de 1981, que fue ratificado por España en enero de 1984, reconocía en su artículo 1, la protección de datos como un Derecho Fundamental<sup>135</sup>.

Años más tarde, la Comisión Europea aprobó la Directiva 95/46/CE, relativa a la protección de personas físicas en lo referido al tratamiento de datos personales y a su libre circulación, cuya principal novedad consistió en, además de tratar de armonizar las legislaciones nacionales, regular la transferencia internacional de esos datos. La mencionada Directiva fue posteriormente desarrollada por el Reglamento 45/2001 del Parlamento Europeo y del Consejo, cuya definición de la protección de datos no varía respecto del recogido en la Directiva.

Posteriormente, la Carta de Derechos Fundamentales de la Unión Europea de 2002 reconoció, si bien con efectos políticos que no jurídicos, el Derecho a la protección de datos de carácter personal en su artículo 8. Su redacción es ya un punto de inflexión, siendo la más detallada y completa hasta entonces: “1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.* 2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.* 3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*” Ya se recogen en el mencionado texto términos hoy habituales en cualquier legislación relativa a la protección de datos pero que entonces no lo eran tanto; fines del tratamiento, consentimiento, acceso o rectificación forman parte de la Carta de Derechos Fundamentales de la Unión Europea y son hoy principios indiscutibles de cualquier legislación relativa al citado ámbito.

Este fue el germen de lo recogido años más tarde en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, hoy en vigor, en el que constan dos preceptos. El primero, de carácter general y que se encarga de reconocer el Derecho subjetivo, señala que “*Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*” El segundo, que establece la obligación y las competencias para el desarrollo legislativo y normativo al respecto, afirma que “*El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión,*

---

108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales”, en *Anuario de la Facultad de Derecho. Universidad de Extremadura*, nº 19, 2002. Págs. 235-252

135 Artículo 1. Objeto y fin: “*El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (“protección de datos”).*”

y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.” Como ahora veremos, estas competencias de las que habla el Tratado han sido desarrolladas ampliamente en los últimos años tanto por la Unión Europea como por los países miembros.

Concretamente, en el ámbito europeo de forma más reciente y de aplicación directa, se aprobó el Reglamento 2016/679 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. Este Reglamento es, quizá, una de las novedades más importantes que en legislación comunitaria se ha producido en la última década. Se trata de una revolución en lo relativo a la privacidad que regula al detalle las obligaciones en este ámbito. El mencionado Reglamento ha sido desarrollado en nuestro País por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que ha mantenido la línea garantista reflejada en el Reglamento Europeo.

Efectivamente, el Derecho a la protección de datos en nuestro País se configura como un Derecho fundamental, y lo hace a través de la Constitución Española que le otorga ese carácter al derecho a la intimidad personal en su art. 18.4, que afirma que *“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”* Si bien es cierto que la protección de datos de carácter personal no es exactamente igual a la intimidad, es obvio que tiene su origen en ella, y se configura como una evolución de este derecho, aunque independiente al mismo. Sin duda, el desarrollo de la tecnología y sus efectos en el ámbito de la intimidad ha sido un factor determinante para ello<sup>136</sup>.

Como ahora veremos, se trata de un Derecho incluido dentro del de la intimidad personal, más bien derivado de este, pero diferenciado del mismo. El contenido del mencionado Derecho Fundamental, sobre el que ahora entraremos en mayor profundidad, consiste, según señala la ya clásica Sentencia del Tribunal Constitucional 39/16 de 3 de marzo de 2016 en su fundamento jurídico 7, *“en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.”*

Como antes ya avanzamos, es importante señalar que el Derecho a la protección de datos de carácter personal es un Derecho distinto e independiente al de la Intimidad. Así, en el primero el objeto no es tanto la vida privada de las personas sino cuestiones relativas al perfil ideológico, personal o ra-

---

136 SOBRINO GARCÍA, I.: “Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos”, en *Revista de Derecho UNED*, núm. 25, 2019, pág. 696

cial de la misma<sup>137</sup>. Ello no impide que el Derecho a la protección de datos incluya también la protección de datos de la vida íntima de las personas, pero su contenido irá más allá, incorporando datos que pudieran ser incluso públicos.

La conocida Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre, cuya doctrina ha sido refrendada recientemente por la Sentencia del Tribunal Constitucional 76/2019 de 22 de mayo, deja claro que el de la protección de datos es un Derecho fundamental distinto del derecho al de la intimidad. Se basa en el otorgamiento a la persona del control sobre sus datos personales y cuyo objeto no es tanto la intimidad de la persona como el perfil ideológico, racial u otro de índole similar.

Así pues, podemos concluir que el Derecho a la protección de datos incluye la protección, no solo de los datos íntimos de una persona, sino también aquellos que, por cualquier motivo, sean públicos y a los que puedan tener acceso terceras personas<sup>138</sup>. Y ello porque cualquier dato personal, independientemente de que este forme parte o no de la esfera íntima de la persona, sea o no público, podría ser empleado por un tercero en beneficio propio y afectar de distintas maneras a cualquier otro de los derechos del afectado. De ahí que, como luego veremos, el consentimiento del titular de los derechos será la piedra angular que permitirá el uso de los datos personales, solo para aquellos que sean autorizados, de terceras personas.

Una vez señalada la diferenciación entre intimidad y privacidad, se hace necesario conocer, no ya el contenido del Derecho Fundamental, sino el concepto de dato personal, que será sobre lo que los ciudadanos puedan solicitar protección ante los tribunales. En este sentido, el Reglamento de la Unión Europea 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

---

137 SANTOS SÁNCHEZ, D. J., *Tratamientos Asociados Al Contexto De La Epidemia: Principios De Protección De Datos, Legitimación Y Actores Intervinientes*, conferencia durante el curso “La protección de datos personales en el marco de la epidemia COVID-19”, Santander, 2020

138 En este sentido, es esclarecedor el fundamento jurídico sexto de la mencionada sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre en el que se afirma al respecto que: “*De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.*”

respecta al tratamiento de datos personales y a la libre circulación de estos datos, del que acabamos de hablar, no se aparta del concepto tradicional que hemos venido viendo de datos personales. Así, el mismo artículo 3 de la Ley Orgánica de Protección de Datos de 1999 contenía ya una definición literalmente igual. De este modo, el Reglamento define en su artículo 4.1 los datos personales como “*toda información sobre una persona física identificada o identificable.*” Se trata de una definición de carácter general en un doble sentido. Por un lado, se trata de una definición aplicable en todo el territorio europeo -tanto es así que la propia Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales no incluye una definición de estos-. Por otro, nos encontramos ante una acepción muy amplia, pues incluye cualquier tipo de información sobre una persona física, siempre que esta esté ya identificada o pueda serlo por medio de los mencionados datos.

Pero ¿Cuáles son esos datos concretos de una persona física? Pues bien, además de los tradicionales datos como la información obtenida de una fotografía, la voz, la imagen, la identificación numérica o incluso la gráfica, durante los últimos años, debido principalmente al avance de la tecnología al que antes hacíamos mención, se han ido incorporando una gran cantidad de nuevos tipos de datos como son los recogidos en el ya comentado artículo 4 del Reglamento General de Protección de Datos que incluyen los biométricos -reconocimiento facial, ocular, dactilar...- o genéticos.

Los primeros de ellos, los biométricos, son definidos por el artículo 4.14 del Reglamento General de Protección de datos como aquellos “*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*” Los segundos, los genéticos, se recogen en el artículo 4.13 del Reglamento General de Protección de datos y son determinados como “*datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona*”.

No podemos ignorar que este tipo de datos son cada vez más utilizados en ámbitos como el laboral, por ejemplo, para fichar a la entrada y la salida de los centros de trabajo con huella dactilar, o incluso en el particular, usando el reconocimiento facial para activar cada vez más aplicaciones móviles. A mayor abundamiento, será habitual que las aplicaciones dotadas con inteligencia artificial usen datos tanto genéticos como biométricos para llevar a cabo distintas acciones.

Es importante señalar que no todos los datos personales tienen el mismo nivel de protección. Así, el artículo 9 del Reglamento General de Protección de Datos establece una serie de categorías con las que se ha de tener especial

cuidado, llegando a prohibir su tratamiento. Algunos de estos datos son relativos al origen étnico o racial, las opiniones políticas o las creencias religiosas<sup>139</sup>. Esa prohibición, aunque tenga un carácter general, contará con algunas excepciones como la que se refiere al interés general o la salud pública en las que nos detendremos con posterioridad por su importancia a la hora de tratar algunas acciones relacionadas con la inteligencia artificial.

Una vez conocido un concepto básico sobre los datos de carácter personal, es necesario detenernos en uno de los elementos principales en esta materia. Me refiero al tratamiento que los terceros podrán hacer de esos datos personales. Que un ciudadano acepte compartir con una empresa o una administración un determinado dato personal, no significa que esa empresa o administración pueda utilizar ese dato para cualquier objetivo. Si yo comparto con una empresa, por ejemplo, mi dirección de correo electrónico para que me remitan información sobre un determinado producto, esa empresa no podrá utilizar ese dato más que para aquello que he autorizado. No podría, por ejemplo, remitirme ofertas genéricas que no tuvieran relación con el producto mencionado. El artículo 4.2 del Reglamento Europeo define ese tratamiento de datos como “*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no...*”<sup>140</sup> Es evidente, por lo tanto, que el uso de la inteligencia artificial, en muchos casos, hará uso de esos datos a través de lo que conocemos como tratamiento.

Aquí llegamos a otro de los elementos centrales de la privacidad: el consentimiento. Será necesario, de conformidad con el artículo 9.2.a del Reglamento Europeo, el consentimiento explícito del afectado para poder tratar los datos de carácter personal. Es decir, cualquier uso que se haga a través de la inteligencia artificial de los datos personales exigirán el “*consentimiento explícito*” del afectado.<sup>141</sup> Aunque en este particular caso nos encontramos ante una circunstancia que hace aún más complejo ese consentimiento, y es que, como señala COTINO HUESO “*con los sistemas de inteligencia artificial y*

---

139 Artículo 9 del Reglamento General de Protección de Datos: “*Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.*”

140 El referido artículo 4.2, tras la definición del tratamiento de datos, señala algunos de estos haciendo referencia expresa a “*la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*”

141 Señala el artículo 9.2.a del Reglamento Europeo que se eximirá de la prohibición del tratamiento de datos de carácter personal tan solo en los casos en los que “*el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados...*”

*decisiones automatizadas es muy difícil consentir respecto de unas finalidades de uso de los datos que por lo general ni se conocen, ni se sospechan.*<sup>142</sup> Así es, más aun teniendo en cuenta que la inteligencia artificial se caracteriza por la capacidad de las máquinas de aprender solas y aplicar ese aprendizaje a sus tareas. Así pues, es posible que pueda llevarse a cabo ese uso sin el consentimiento del afectado siempre y cuando, como ahora veremos más detenidamente, los datos estén anonimizados o seudonimizados.

Es por ello por lo que será fundamental que cualquier procedimiento que lleve aparejado el uso de inteligencia artificial o bien contenga una clara advertencia para aquellos que puedan verse afectados por el mismo, o bien, a través de distintos medios, se desvinculen los datos de la persona a través de la anonimización o de la seudonimización. Esta necesidad ya se recoge en la Carta de Derechos Digitales que, como ya hemos comentado, va aún más allá y exige, no solo que se informe a los ciudadanos de que las decisiones o el procedimiento se llevarán a cabo a través de la inteligencia artificial, sino que, además, tendrán derecho a *“no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, que produzcan efectos jurídicos o les afecten significativamente de modo similar, salvo en los supuestos previstos en las Leyes.”*<sup>143</sup> Y esto es un elemento muy importante, puesto que garantiza a los ciudadanos el que, a pesar de que puedan tomarse decisiones sobre su persona a través de un algoritmo de inteligencia artificial, puedan a su vez ser revisadas por personas físicas.

Así, por ejemplo, en el ámbito laboral, existirá la obligación, según el apartado 17.4 de la Carta de Derechos Digitales, de informar expresamente a los trabajadores del uso de sistemas de inteligencia artificial.<sup>144</sup> A continuación, con motivo del estudio del artículo 22 del Reglamento General de Protección de Datos, lo analizaré con mayor detenimiento.

## **2. PRIVACIDAD, PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL**

Sin lugar a duda, la protección de datos también tendrá que adaptarse a la nueva realidad que impone la inteligencia artificial. Mejor dicho, la inteligencia artificial tendrá que, por defecto y desde el diseño, establecer procedimientos para que su aplicación sea compatible con el respeto a la privacidad. No podemos obviar que el tratamiento de datos, con el avance de la inteligencia artificial, aumentará de manera muy notable convirtiéndose

---

142 COTINO HUESO, L.: “Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales”, en *Dilemata*, núm. 24, 2017, pág. 145

143 Apartado 25. C de la Carta de Derechos Digitales

144 La Carta de Derechos Digitales, sometida en este momento a consulta pública, establece en su apartado 17.4 que *“se informará a los representantes de los trabajadores y las personas directamente afectadas sobre el uso de la analítica de datos o sistemas de inteligencia artificial en la gestión, monitorización y procesos de toma de decisión en materia de recursos humanos y relaciones laborales”*

en un uso masivo y veloz. Lo mismo sucederá con los riesgos que lleva aparejados. A mayor uso de datos, especialmente con un volumen tan amplio, mayor posibilidad de que se pueda violar la privacidad de los ciudadanos.

El propio Parlamento Europeo, de manera reciente, se ha manifestado en este sentido en su Recomendación a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas. En la citada recomendación afirma que “*el uso de datos, incluidos los datos personales como los datos biométricos, resultantes del desarrollo, despliegue y utilización de la inteligencia artificial, la robótica y las tecnologías conexas están aumentando rápidamente, lo que pone de relieve la necesidad de respetar y hacer cumplir los derechos de los ciudadanos a la intimidad y la protección de los datos personales de conformidad con el derecho de la Unión*”<sup>145</sup>.

Como bien señala DE MONTALVO, aplicado el uso masivo de datos al ámbito sanitario, “*En el momento actual, la explotación masiva de datos genera ciertos riesgos en relación con los derechos de los individuos, pero, por otro lado, ofrece verdaderas posibilidades de curación o prevención también para la comunidad*”<sup>146</sup>. Las autoridades europeas, aunque han alabado las ventajas del uso de la inteligencia artificial, también han alertado de algunos de los posibles usos indebidos en este ámbito, como podrían ser la vigilancia en masa o la violación de las garantías procesales<sup>147</sup>. Volvemos, nuevamente, a reiterar la necesidad de lograr ese ansiado equilibrio entre la potencialidad de la inteligencia artificial y el respeto a la privacidad.

Si antes de que la inteligencia artificial formase parte de nuestro día a día ya se generaban importantes riesgos, más aún se producirán ahora, cuando su uso se ha normalizado en múltiples aplicaciones. Ello interferirá, sin duda alguna, en el cumplimiento de uno de los principios generales en este ámbito como es la minimización de datos. Este principio, según lo establecido en el artículo 5.c) del Reglamento General de Protección de Datos, implica que los datos sean “*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.*” Como señala acertadamente RIESTRA HERRERA, la minimización de datos será difícilmente compatible con el uso masivo de datos que conlleva la inteligencia artificial<sup>148</sup>.

---

145 Vid. Recomendación del Parlamento Europeo a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 20 de octubre de 2020, recomendación núm. 63

146 Cfr. DE MONTALVO JÄÄSKELÄINEN, F.: “Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del big data”, en *Revista de Derecho Político*, núm. 106, 2019, pág. 52

147 Vid. Recomendación del Parlamento Europeo a la Comisión... Op. cit. recomendación núm. 66

148 Vid. RIESTRA HERRERA, E.: *Privacidad en el diseño de la inteligencia artificial*, Editado por Riestra Abogados, 2017, pág. 106

Es por ello por lo que se tendrán que desarrollar técnicas preventivas que permitan, entre otras cosas, la seudonimización y anonimización de datos.<sup>149</sup> Estas dos técnicas han sido avaladas por el Grupo de trabajo sobre protección de datos del artículo 29 que considera como una buena práctica que los responsables del tratamiento de los datos utilicen las técnicas de anonimización y seudonimización de las que ahora hablaré con mayor detalle<sup>150</sup>.

Estos dos principios, el de seudonimización y anonimización de datos, han sido ya recogidos en la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial. Concretamente su artículo 10.5 los plantean como necesarios para proteger con garantías adecuadas los derechos y libertades fundamentales de las personas físicas en los casos de reutilización y de protección de la intimidad<sup>151</sup>.

Tal es la importancia del tema que estamos ahora tratando que la propia Agencia Española de Protección de Datos ha elaborado una guía monográfica para la Adecuación al RGPD de los tratamientos que incorporan Inteligencia Artificial, en la que se redonda en esta idea de hacer compatible el uso de la inteligencia artificial con la implementación de garantías para la protección de datos personales. Se concluye en el citado documento que “*la puesta en el mercado, para entidades y consumidores en general, de tratamientos que incluyan soluciones basadas en tecnologías disruptivas, como las basadas en componentes IA, exige que se implementen garantías de calidad y seguridad*”<sup>152</sup>.

Si la privacidad se ha convertido en nuestros días en una cuestión fundamental, en todo lo relacionado con la inteligencia artificial lo es aún más porque ésta se basa en casi todas las ocasiones en el acceso de datos detallados y personales<sup>153</sup>. La dificultad estribará en encontrar el equilibrio

---

149 SÁNTOS GONZÁLEZ, M.J.: “Regulación legal Op. cit, pág. 34

150 Vid. “Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679”, *Grupo de trabajo sobre protección de datos del artículo 29, Comisión Europea*, 2016 pág. 36. Accesible en <https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf>

151 En la medida en que sea estrictamente necesario para garantizar la supervisión, la detección y la corrección de sesgos en relación con los sistemas de IA de alto riesgo, los proveedores de dichos sistemas podrán tratar las categorías especiales de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas, incluidas las limitaciones técnicas a la reutilización y el uso de medidas de seguridad y de preservación de la intimidad de última generación, como la seudonimización, o el cifrado cuando la anonimización pueda afectar significativamente a la finalidad perseguida

152 Cfr. Agencia Española de Protección de Datos. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020, pág. 49

153 Vid. SAIF, I. y AMMANATH, B.: “Trustworthy AI is a framework to help manage... Op. cit.

necesario entre el desarrollo y adecuado uso de la inteligencia artificial, por un lado, y la protección de los datos de carácter personal por otro.

A pesar de que el RGPD no menciona de forma expresa la inteligencia artificial, sí que dedica dos artículos, el 21 y el 22, a lo que denomina *decisiones individuales automatizadas*. Son, en definitiva, una de las aplicaciones habituales de la inteligencia artificial. A ello, por su importancia, ha prestado una especial atención la Comisión Europea a través de una completa guía de Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 que contienen una serie de recomendaciones de carácter técnico.

El artículo 21 del citado reglamento, relacionado con la publicidad o mercadotecnia, permite al interesado oponerse al tratamiento de sus datos. Sin duda, el más relevante para nuestra investigación es el artículo 22 del citado reglamento. En este apartado se establece por primera vez el derecho de todo ciudadano, respecto a sus propios datos, a “*no ser objeto de una decisión basada únicamente en el tratamiento automatizado... que produzca efectos jurídicos*”, salvo para los casos en los que sea necesario para celebrar un contrato con el responsable del tratamiento, exista autorización por la legislación correspondiente o existiese consentimiento expreso del interesado. Sobre este particular se ha pronunciado hace escasas fechas el Parlamento Europeo, señalando que “*toda decisión adoptada por la inteligencia artificial, la robótica o las tecnologías conexas en el marco de las prerrogativas del poder público debe estar sujeta a una intervención humana significativa y a las debidas garantías procesales*”<sup>154</sup>.

A este respecto, MATURO SERNA señala dos posibles carencias en la normativa europea.<sup>155</sup> Por un lado, que este límite opera solamente en el caso en la que decisión sea tomada únicamente por la inteligencia artificial, excluyendo por lo tanto los casos en los que en la decisión participen tanto un ser humano como la inteligencia artificial. Por otro, advierte de la problemática que podría generarse en los casos en los que existan decisiones automatizadas que usen los datos personales de un ciudadano pero que no tengan consecuencias jurídicas para él<sup>156</sup>.

---

154 Vid. Recomendación del Parlamento Europeo a la Comisión... Op. cit. recomendación núm. 69

155 Vid. MATURO SERNA, A.: “Inteligencia artificial y privacidad: un encaje problemático.”, en *La Ley*, núm. 2, 2019, págs. 2 y 3

156 Para ilustrarlo utiliza el siguiente ejemplo: “*¿Qué pasaría en los casos en los que las decisiones automatizadas sean tomadas por una máquina que tiene como único fin el de medir el grado de satisfacción de un cliente en un restaurante, captando los rasgos de su expresión facial? En este caso, no existirán «efectos jurídicos» para el comensal (no se le denegará el acceso en futuras ocasiones, ni se le cobrará un precio distinto en función de su grado de satisfacción), sino que, simplemente, se medirá eso: su grado de satisfacción. Ergo, no existiendo «efectos jurídicos» para el interesado, éste tampoco podrá exigir no verse sometido a este escrutinio por parte la IA.*” Cfr. MATURO SERNA, A.: “Inteligencia... Op. cit. pág. 3

El primero de los problemas planteados entiendo que es salvable, puesto que la garantía exigible es precisamente la participación de un ser humano en la toma de la decisión. Para que se considere que existe participación de un ser humano en ese proceso bastará con que este revise o use los datos generados con la aplicación de la inteligencia artificial y no tendrá cabida en esta acepción su uso indiscriminado y de forma automática sin participar en lo más mínimo en la decisión<sup>157</sup>.

Una garantía que evitará casos como el sucedido recientemente en el hospital estadounidense de Stanford en el que, durante la pandemia del COVID19, fue un algoritmo basado en inteligencia artificial el que cometió un grave error al decidir a qué miembros del hospital vacunar en primer lugar. El algoritmo que se usó priorizó a los trabajadores que se suponía podían tener un mayor riesgo de infecciones por COVID19, pero usando únicamente factores como la edad y sus antecedentes médicos, sin incluir si los trabajadores tenían o no relación directa con pacientes COVID19. El resultado fue que la mayoría de los primeros 3.000 trabajadores que iban a vacunar atendían el teléfono o realizaban tareas que no implicaban una relación con pacientes. Por el contrario, tan solo siete de los que se iban a vacunar en esta primera ronda eran médicos que se encontraban en primera línea en la lucha contra la pandemia. Ello provocó graves protestas por lo que el hospital tuvo que recurrir a otro sistema, con la participación exclusivamente humana en este caso, para decidir finalmente a quién se vacunaría y en qué orden<sup>158</sup>. Aunque, en puridad, nos encontramos ante lo que es un error humano puesto que los algoritmos fueron diseñados por una persona y no fueron diseñados exclusivamente por el ordenador en base al aprendizaje autónomo de este. Sea como fuere, esta situación no podría producirse en nuestro país pues, como acabamos de ver, esas decisiones no pueden ser tomadas únicamente por la aplicación, sino que tienen que contar con la participación humana, bien sea revisando el resultado de la propuesta elaborada por la inteligencia artificial, bien sea participando en la elaboración de la propuesta definitiva. Entiendo que el uso de este tipo de herramientas son una ayuda indispensable, pero hubiese sido lógico y seguro comprobar el resultado del algoritmo antes de que este tenga efectos, en este caso, con el personal del hospital. Como digo, una garantía para evitar situaciones indeseables que pudiesen generar graves perjuicios a los afectados.

El segundo de los interrogantes, el relativo a la necesidad de que la toma automatizada de decisiones tenga efectos jurídicos para establecer la obli-

---

157 Vid. SÁNCHEZ DEL CAMPO REDONDET, A.: “Inteligencia artificial y privacidad”, *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, LÓPEZ CALVO, J. (Coord.), Ed. Bosch, 2019, págs. 983 a 985

158 WAMSLEY, L. (2020). Stanford Apologizes After Vaccine Allocation Leaves Out Nearly All Medical Residents. *NPR*. Accesible en <https://www.npr.org/sections/coronavirus-live-updates/2020/12/18/948176807/stanford-apologizes-after-vaccine-allocation-leaves-out-nearly-all-medical-resid?t=1609683461837>

gatoriedad de la participación del ser humano en la decisión, sí me genera muchas más dudas, porque no deja de tratarse de un concepto jurídico indeterminado. La ya mencionada guía de directrices sobre decisiones individuales automatizadas define estos efectos jurídicos como la exigencia de que “*la decisión, basada únicamente en el tratamiento automatizado, afecte a los derechos jurídicos de una persona...-o- que afecte al estatuto jurídico de una persona o a sus derechos en virtud de un contrato*”<sup>159</sup>. Es cierto que la decisión tomada por la inteligencia artificial no tendrá efectos jurídicos sobre esa persona en concreto, pero eso no obsta para que, por ejemplo, su opinión se vea escrutada y sea utilizada para tomar una decisión que sí podría tener otro tipo de efectos, aunque no jurídicos, con terceras personas. Imaginemos una aplicación basada en el uso de tecnología con inteligencia artificial, que sea capaz de captar por el tono de voz de una persona, la satisfacción con el uso de, por ejemplo, un establecimiento hotelero. Esa información podría ser usada en aplicaciones como *Booking* o cualquier otra similar, para establecer una determinada puntuación que haría que otros usuarios pudieran ser acudir al mencionado establecimiento, con la importancia que este tipo de decisiones tiene, por ejemplo, en el mercado.

En esta misma línea, el apartado XXIII de la Carta de Derechos Digitales, sometida a consulta pública y que se dedica a los Derechos de los ciudadanos ante la inteligencia artificial, establece que “*las personas tienen derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, incluidas aquellas que empleen procedimientos de inteligencia artificial*”. Así pues, se trata del primer elemento en el que la protección de datos limita el uso de la inteligencia artificial, aunque no el único.

El mismo apartado de la citada Carta de Derechos Digitales, en su punto 3, establece otra exigencia, que no es otra que la obligación de informar del uso de esta a los ciudadanos. Así, señala que “*se deberá informar a las personas sobre el uso de sistemas de Inteligencia Artificial que se comuniquen con seres humanos utilizando el lenguaje natural en todas sus formas, garantizándose en todo caso la asistencia por un ser humano a solicitud de la persona interesada*.” Encontramos aquí otro de los pilares para lograr ese adecuado equilibrio, que no es otro que el disponer de una información transparente y clara, que permita a los ciudadanos conocer el fin del tratamiento que las aplicaciones dotadas con inteligencia artificial harán con sus datos. Esa información deberá ser lo suficientemente amplia como para que cualquier persona pueda autorizar y consentir el tratamiento que pretende llevar a cabo el responsable de los mismos.

Pero esa información que mencionamos no será sencilla, puesto que será difícil determinar los fines a priori cuando nos encontremos ante el uso de la inteligencia artificial. Especialmente complejo será el uso secundario que, sin el consentimiento expreso del titular de los datos, se le vaya a dar. De este

---

159 Cfr. “Directrices sobre... Op. cit. pág. 23

modo hay quien sostiene que ese uso secundario, “*cuando el interés general sea relevante, no exigiría la obtención de un nuevo consentimiento informado*”<sup>160</sup>. En mi opinión, tan solo sería aceptable en dos supuestos: En primer lugar, cuando los datos se utilicen de manera seudonimizada. Es decir, cuando esos datos se hayan separado completamente de la identidad de aquel que cedió los datos y, siempre y cuando, se hubiese advertido en la información originaria trasladada a este. El segundo de ellos, cuando nos encontremos ante un caso de interés general o de protección para la salud.

Pero reitero mi preocupación por el hecho de que ese interés general lo sea de verdad, y no una simple excusa para generalizar la posibilidad de usar los datos sin consentimiento del afectado para fines distintos. Por eso y también porque ese uso cumpla bien con la anonimización de los datos o la seudonimización de los mismos. Es necesario evitar casos como el sucedido recientemente en Singapur, donde las fuerzas y cuerpos de seguridad podrán tener acceso los datos de rastreo de la aplicación que las autoridades crearon para la lucha contra el COVID19 para ayudar en sus investigaciones penales. Esto, en mi opinión, se trata de una clara violación del derecho a la privacidad sin justificación ética ni legal alguna<sup>161</sup>.

Comparto la postura de por MIRALLES LÓPEZ cuando afirma que “*el reto y la dificultad será crear un conjunto de datos protegidos, que, sin identificar directamente a las personas, resulten útiles a la finalidad del posterior tratamiento*”<sup>162</sup>. Se trata precisamente de eso; de ser capaces de diseñar un proceso de seudonimización, del que ahora hablaré con mayor profundidad, que nos permita usar datos que puedan tener interés para otros fines distintos a los consentidos por el titular de los mismos, pero siempre garantizando que esos datos no podrán identificarse con la persona a la que pertenecen y que, en el momento de prestar su consentimiento inicial, conozca su posible uso en las condiciones relatadas ahora.

Como he señalado, la política en esta área tiene que estar guiada por un diseño basado en la prevención. Y para ello serán fundamentales los dos principios a los que me vengo refiriendo, la anonimización y la seudonimización, sobre los que ha de girar la política de protección de datos en el ámbito de la inteligencia artificial. Sobre el primero, que consiste en la separación absoluta y definitiva entre la identificación personal y los datos obtenidos, el RGPD no realiza definición alguna. Aunque sí se refiere a él en el considerando 26 del mismo, para afirmar que los principios básicos de la protección

---

160 Vid. DE MONTALVO JÄÄSKELÄINEN, F.: “Una reflexión ... Op. cit., pág. 63

161 YU, E.: Singapore police can access COVID-19 contact tracing data for criminal investigations. *Zdnet*. 4 de enero 2021, accesible en <https://www.zdnet.com/article/singapore-police-can-access-covid-19-contact-tracing-data-for-criminal-investigations/>

162 Cfr. MIRALLES LÓPEZ, R.: “Desvinculando datos personales: Seudonimización, Desidentificación y Anonimización”, en *Revista de la Sociedad Española de Informática y Salud*, núm. 122, 2017, pág. 9

de datos no le son de aplicación puesto que se trataría de “*información que no guarda relación con una persona física identificada o identificable*”<sup>163</sup>.

Desde hace ya años, los investigadores y científicos vienen solicitando con insistencia la posibilidad de utilizar datos almacenados, no identificados con una persona en concreto, para fines distintos de los que se recogieron en su momento<sup>164</sup>. La única opción, fuera de los casos de interés general sobre los que hablaremos con mayor amplitud a continuación, para dar respuesta a esta demanda pasa por anonimizar o seudonimizar esos datos.

La propia Agencia Española de Protección de Datos señala que en el proceso de anonimización “*se deberá producir la ruptura de la cadena de identificación de las personas*”<sup>165</sup>. Así pues, si los datos obtenidos se almacenan y gestionan de manera que hacen imposible identificar a la persona física que hay detrás de los mismos, la protección de la privacidad estará garantizada. Ello hace que la anonimización de datos sea una herramienta ideal para el tratamiento de datos por aplicaciones que se basen en el uso de la inteligencia artificial. Cuestión distinta, y responsabilidad de los encargados del tratamiento de datos, será garantizar esa anonimización durante todo el proceso, de principio a fin. Sin duda puede tratarse de una técnica en ocasiones compleja, pero que se configura como una de las principales herramientas para hacer compatibles la privacidad y la inteligencia artificial<sup>166</sup>.

La Unión Europea ha manifestado su preferencia por este principio en el uso masivo de datos, al señalar que, en este ámbito, deben usarse los “*datos anonimizados y agregados cuando sea posible.*” Así lo establece en su recomendación número 15 relativa a los aspectos relativos a la intimidad y la protección de datos derivados del uso de las aplicaciones móviles recogidas en la Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en

---

163 Señala el considerando 26 del RGPD que “*Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.*”

164 Vid. KOKKINAKIS, D.: “Complementary Methods for De-identifying Sensitive Data with a focus on Clinical Discourse”, en *Procesamiento del Lenguaje Natural*, núm. 45, 2010, pág. 243

165 Agencia Española de Protección de Datos: *Orientaciones y Garantías En Los Procedimientos De Anonimización De Datos Personales*. 2016, pág.2 Accesible en <https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf>

166 Afirma en este sentido PÉREZ SANZ que “*Existen muchas y muy variadas metodologías de anonimización, y es muy posible que sea necesario combinar varias de ellas para asegurar la completa disociación en un proyecto Big Data. En cualquier caso, debe tenerse en cuenta que la anonimización debe asegurarse de principio a fin, es decir, en todos y cada uno de los procesos y tratamientos de información específicos asociados al proyecto en cuestión...*” Vid. PÉREZ SANZ, C.: “Aspectos legales del Big Data”, en *Revista de estadística y sociedad*, núm. 68, 2016, pág. 20

particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados.

Es por ello por lo que la anonimización de los datos en el uso de tecnología con inteligencia artificial sería una buena herramienta para evitar la violación del derecho a la privacidad. Es, quizá, la fórmula más adecuada para conseguir ese difícil equilibrio entre el avance de una tecnología como la inteligencia artificial y la protección del derecho a la privacidad, que en muchas ocasiones pueden colisionar.

Por el contrario, el artículo 4.5 del RGPD sí que define el otro principio que se debe de configurar como clave en la protección de datos, el de la seudonimización, como “*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.*” Pero, al revés que sucedía con los datos anonimizados, en este caso sí que entra en juego la política de protección de datos, por poderse ver afectada la privacidad de los ciudadanos. Así, como señala TIMÓN HERRERO, los datos en estos casos deberían de incluir “*un acceso y un tratamiento lícito, leal y transparente, con una finalidad limitada, respetando los parámetros de la proporcionalidad, el principio de exactitud de los datos y su conservación limitada*”<sup>167</sup>. Sería pues recomendable que, en aquellos casos en los que no fuera posible la anonimización en el uso de la inteligencia artificial, se optase por la seudonimización. Como bien señala BLÁZQUEZ AGUDO, esta técnica se dispone como la forma ideal para “*garantizar la seguridad de los datos personales frente a ataques de terceros*”<sup>168</sup>.

Sería necesario, como bien señala el artículo 25 del RGPD, incluir el principio de seudonimización desde el diseño mismo de la política de protección de datos, y por defecto, en el uso de cualquier herramienta que cuente con inteligencia artificial.<sup>169</sup> Ello garantizaría poder usar determinados datos sin que, con carácter general, se tuviese acceso a la identificación personal. Nos encontraríamos ante una herramienta muy útil que permitiría, salvaguardando la privacidad de las personas físicas, el acceso y

167 Vid. TIMÓN HERRERO, M.: “Protección de datos de carácter personal y crisis sanitaria (Covid 19)”, en *elderecho.com*, 7 de agosto de 2020

168 Cfr. BLÁZQUEZ AGUDO, E.M.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Ed. CISS, 2018, pág. 187

169 El artículo 25 del Reglamento General de Protección de Datos establece: “*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*”

el uso de datos que podrían llegar a ser clave en casos como el de la protección de la salud pública. Así lo ha recogido la Ley Orgánica de Protección de Datos en cuya disposición adicional decimoséptima, apartado 2.d., permite el uso de datos personales seudonimizados para fines relacionados con la salud<sup>170</sup>.

En definitiva, a pesar de que parte de la doctrina entiende que ni el RGPD ni el resto de la legislación actual en materia de protección de datos es suficiente para responder ante los retos aparecidos con la inteligencia artificial<sup>171</sup>, yo me inclino por pensar que sí lo es, lo que no obsta para que las autoridades públicas deban seguir teniendo en cuenta políticas específicas de protección de la privacidad en el desarrollo de las distintas normativas relacionadas de una forma u otra con esta materia. En esta misma línea, y a pesar de que no se ha descartado una futura reforma, tanto el Parlamento Europeo como la Comisión Europea han optado, no por una reforma legislativa, sino por impulsar el establecimiento de directrices específicas directrices sobre la aplicación del Reglamento Europeo de Protección de Datos en el ámbito de la inteligencia artificial, así como de otros posibles avances tecnológicos<sup>172</sup>.

### 3. INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS EN TIEMPOS DE PANDEMIA

Mención especial merece la aplicación de la inteligencia artificial en procesos relativos a la protección de la salud. De hecho, algunos autores reivindican la necesidad de contar con una legislación específica para este ámbito que permita, de una forma clara y segura, el uso de datos personales para fines distintos para los que inicialmente fueron cedidos.<sup>173</sup> No podemos ob-

---

170 “El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá: 1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. 2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación”

171 Así se ha manifestado entre otros MATURO SENRA, sosteniendo que “los actuales instrumentos jurídicos (in primis, el brevemente analizado art. 22 RGPD) no parecen responder a los ambiciosos retos planteados por los avances tecnológicos”, Vid. MATURO SERNA, A.: “Inteligencia... Op. cit., pág. 4

172 Vid. Recomendación del Parlamento Europeo a la Comisión... Op. cit. recomendación núm. 50

173 Así se ha manifestado SARRIÓN ESTEVE, que sostiene que a este respecto que “las tendencias actuales en el procesamiento de datos de salud incluyen grandes desafíos de datos, inteligencia artificial e Internet en las cosas (IO), y por lo tanto necesitamos un marco legal mejor y más claro de procesamiento de datos sanitarios para la investigación biomédica a nivel europeo y nacional.” Cfr. SARRIÓN ESTEVE, J.: “The problem of the consent for the processing of health data, particularly for biomedical research purposes, from the perspective of fundamental rights protection in the Digital Era”, en *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, núm. 48, 2018, pág. 131

viar que con la pandemia del COVID19 nos hemos encontrado ante una circunstancia extraordinaria en la que se han tenido que tomar medidas excepcionales tanto de seguridad como de protección de los ciudadanos.

Como ya hemos señalado, y como sucede con cualquier otro Derecho, el de la protección de datos cuenta también con ciertos límites. Uno de esos límites es precisamente el de la protección de la salud pública. Hemos de ser conscientes de que, en situaciones como la vivida durante la pandemia del COVID-19, puede hacerse necesario limitar ese Derecho, siempre con garantías suficientes de que lo sea de manera temporal y proporcionada, sea motivado por la protección de otro derecho fundamental y se establezca, como ahora veremos, mediante la correspondiente ley orgánica. Pero esa limitación no puede convertirse en optar por una -salud pública- u otra -privacidad-, como si fuesen en todo caso incompatibles. Como afirma COTINO HUESO, “*es muy importante no simplificar, polarizar y reducir la cuestión a una renuncia a la privacidad para mantener la vida o la salud*”<sup>174</sup>.

Hemos de recordar que, en el presente caso, para tratar de contener la pandemia el Gobierno decretó el Estado de Alarma, lo que muchos entendieron que permitiría suspender algunos derechos fundamentales. Pero ello no es así ya que el artículo 55 de la Constitución Española impide, al tratarse de un Derecho fundamental, la suspensión de los mismos y, por lo tanto, tampoco el de la protección de datos, salvo para los casos relacionados con los estados de excepción o de sitio y siempre a través de la correspondiente ley orgánica<sup>175</sup>. Así lo ha señalado el Tribunal Constitucional en su sentencia 83/2016 de 28 de abril de 2016 en la que afirma que “*a diferencia de los estados de excepción y sitio, la declaración del estado de alarma no permite la suspensión de ningún derecho fundamental, aunque sí la adopción de medidas que pueden suponer limitaciones o restricciones a su ejercicio*”. Así, no podría suspenderse, pero sí limitarse, y siempre a través de la correspondiente Ley Orgánica, algo que no ha sucedido en el presente caso.

---

174 COTINO HUESO, L.: “Inteligencia Artificial y vigilancia digital contra el Covid-19 y contra la privacidad. El diablo está en los detalles”, en Boletín Español de Estudios Estratégicos, 23 de abril de 2020, pág. 3

175 El artículo 55 de la Constitución Española establece que: “*1. Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción. 2. Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las leyes.*”

Distintas normativas reconocen esas limitaciones. De este modo, el artículo 8.2 del Convenio de Roma permite esas excepciones respecto a la autoridad pública siempre que la *“injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.”* Así lo ha señalado también la ya mencionada Sentencia del Tribunal Constitucional de 22 de mayo de 2019 al afirmar que *“Como los demás derechos, el derecho fundamental a la protección de datos personales no tiene carácter absoluto. Puede ser restringido por medio de la ley, siempre que ello responda a un fin de interés general, y los requisitos y el alcance de la restricción estén suficientemente precisados en la ley y respeten el principio de proporcionalidad.”*

Hay autores como DE MONTALVO que son muy contundentes en cuanto a la necesidad de limitar la protección de datos en pro de la salud. Mantiene este autor que *“no se trata de poner riesgo o sacrificar la intimidad y el derecho a la confidencialidad y protección de datos en pos de otros valores y derechos de no tal trascendencia constitucional e impacto en la dignidad del ser humano como aquellos, sino de limitarlos en pos de la protección de la vida e integridad de terceros”*<sup>176</sup>. Aunque de sus palabras pudiese deducirse la necesidad de establecer una limitación genérica, duradera en el tiempo, lo que viene a proponer es la aplicación de la seudonimización como fórmula para dar cumplimiento a la proporcionalidad. Comparto, como ya he señalado anteriormente, la necesidad del uso de la seudonimización en el uso masivo de datos por la inteligencia artificial, pero también creo necesario ir algo más allá, siendo necesario en origen el consentimiento del titular de los derechos para el uso de sus datos seudonimizados. De este modo, me inclino más por una ponderación que permita conciliar ambos derechos y que en aquellos casos en lo que esto no sea posible, la limitación sea siempre temporal, proporcional y se encuentre garantizada por una legislación específica. No se trata pues de no aprovechar los medios que nos da la inteligencia artificial, sino de buscar la vía para hacerlo, respetando la privacidad con política de protección de datos específica y diseñada para hacerlos compatibles.

Así pues, para restringir el derecho a la protección de datos hay que contar con la existencia de dos límites. Por un lado, que responda a un fin constitucionalmente legítimo o, como sucede en el caso de la pandemia COVID-19, tener como objetivo proteger un bien *“constitucionalmente relevante”* como es la salud, recogido en el artículo 43 de la Constitución Española<sup>177</sup>. Por otro, cualquier injerencia del Estado en un Derecho fundamental, como lo es el de la protección de datos, ha de ser proporcional, temporal y ha de

---

176 Vid. DE MONTALVO JÄÄSKELÄINEN, F.: “Una reflexión ... Op. cit., pág. 54

177 Artículo 43 de la Constitución Española: “1. Se reconoce el derecho a la protección de la salud. 2. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios. La ley establecerá los derechos y deberes de todos al respecto

contar con la correspondiente habilitación legal, como señala el artículo 53.1 de la Constitución Española al establecer que “*Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades...*”.

Sin duda, tras la catastrófica situación provocada por el COVID-19, las autoridades públicas tuvieron que tomar decisiones que limitaban el derecho a la protección de datos de los ciudadanos. Así, al igual que sucede con el ya mencionado artículo 8 del Convenio de Roma, el art. 9.4 del Reglamento General de Protección de Datos, redundando en esas posibles limitaciones a la privacidad al señalar expresamente que “*Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.*” Así pues, no cabe duda de que la crisis sanitaria provocada por la pandemia del COVID-19 es uno de los casos en los que la limitación, de manera proporcional y temporal, del derecho a la protección de datos es factible, pero cumpliendo con las exigencias legalmente establecidas.

A este respecto es importante recordar que estas medidas en las que se recojan los límites ahora mencionados tienen que ser fijadas a través de las correspondientes leyes orgánicas, en las que se han de incluir los presupuestos concretos, las garantías que han de establecerse y unas medidas proporcionales, entendiendo como tales la idoneidad de las mismas, la necesidad y la proporcionalidad. Esa temporalidad en la toma de medidas excepcionales es uno de los elementos básicos de los principios de precaución y prevención, y se establece igualmente en el artículo 4.2 del Código civil, que afirma que “*Las leyes penales, las excepcionales y las de ámbito temporal no se aplicarán a supuestos ni en momentos distintos de los comprendidos expresamente en ellas.*” El razonamiento parece lógico, las medidas adoptadas en y para una situación excepcional no pueden extenderse a una situación normal. Deben de ser limitadas en el tiempo. Pensemos, por ejemplo, en el uso de cámaras de reconocimiento facial a la entrada de las grandes superficies o térmicas en los comercios. Son medidas que tienen sentido en un momento determinado, excepcional, pero que deben de desaparecer en cuanto la situación de excepcionalidad termine.

Pongamos un ejemplo para tenerlo más claro. Ya hemos comentado la polémica suscitada en Corea del Sur por el uso de una aplicación de rastreo, dotada con inteligencia artificial, que permitía conocer la ubicación de las personas infectadas por el coronavirus COVID19. Ello provocó que se conociera que un foco había surgido en un bar que frecuentaban homosexuales y generó un amplio debate porque, como es lógico, la orientación sexual de cualquier persona es uno de los datos personales que más protección deben de tener. Es aquí donde se encuentra el principal debate: Cómo equilibrar la protección de la salud a la vez que protegemos los datos personales de los ciudadanos.

En otras palabras, la pregunta que hemos de hacernos es si los datos personales pueden ser usados para un fin distinto a aquel para el que se habían cedido en casos excepcionales como el que acabamos de señalar relativo a la protección de la salud. Dicho de otro modo, ¿Podrían los estados usar los datos personales, sin el consentimiento del interesado, para, entre otras cosas, luchar contra una pandemia como la que sufrimos con el Covid19? ¿Podemos conocer el lugar del brote y quienes son las personas que estaban en aquel lugar en ese determinado momento? ¿Sería proporcional ese uso? La respuesta, aunque afirmativa, ha de ser matizada para hacer compatible la protección de la salud con la protección de datos. Una protección que tiene que estar basada en el establecimiento de unas obligaciones claras desde su diseño para el encargado del tratamiento de los datos. Unas obligaciones que han de pasar porque ese diseño esté basado en una política la prevención con los dos principios ya mencionados.

Es el propio RGPD el que permite algunas excepciones, como la relativa precisamente a la protección de la salud pública, incluida en el Considerando 54 del mencionado reglamento establece que *“El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública...”* Así lo ha reiterado recientemente la Agencia Española de Protección de Datos, en un informe de 17 de marzo de 2020, en el que reafirma la posibilidad de que se traten datos personales relativos a la salud sin que participe el consentimiento de los interesados, siempre que nos encontremos ante una situación de interés público relacionado con la salud pública.

Esta reflexión tiene su plasmación práctica en el artículo 9.2.i del RGPD por el que se exime de la prohibición del tratamiento de datos personales en el caso de que fuera este necesario *“por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios...”*.

Algo similar sucede en lo que respecta a la investigación científica, en la que también se permite cierta flexibilidad aunque esta no sea tan amplia como lo es para la protección de la salud pública. Así, el considerando 159 del RGPD señala que en este ámbito las normas han de ser interpretadas de manera amplia, lo que no obsta para que sea necesaria la existencia de un consentimiento previo por parte del interesado para que sus datos sean tratados en una investigación científica<sup>178</sup>. Así, entiendo que, si un ciudadano presta su consentimiento para ceder sus datos personales como voluntario para probar la eficacia y seguridad de una determinada vacuna, esos datos

---

178 Señala el Considerando 159 del RGPD que *“El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado.”*

podrían utilizarse para un fin distinto al original siempre que fuese en beneficio del interesado o por motivos de salud pública.

Eso no obsta para que el tratamiento de esos datos se lleve a cabo tomando todas las precauciones exigibles para que este tratamiento esté sujeto a las medidas necesarias para proteger los derechos y libertades de las personas físicas. Así, el mencionado artículo 9.2.i del RGPD establece que será exigible, en base al Derecho de la Unión Europea o de sus Estados miembros, el establecer “*medidas adecuadas y específicas para proteger los derechos y libertades del interesado.*” Y ahí es donde está el equilibrio. Hemos de hacer compatible la protección de datos con el uso de estos en casos excepcionales, garantizando el uso de los datos va a llevar aparejada la anonimización o la seudonimización de los mismos, como hemos venido sosteniendo. Dicho de otro modo, que el Estado tenga acceso a este tipo de datos de manera excepcional y en casos graves para proteger la salud de los ciudadanos, debe de hacerse con las máximas garantías de protección de esos datos. Como acertadamente señala PIÑAR, no se trata de que la protección de datos prohíba el uso de estos, “*sino que marca la línea que indica cómo deben hacerse las cosas*”<sup>179</sup>. En este caso con proporcionalidad y precaución tratando de garantizar por un lado la salud pública y, por otro, la privacidad de todos los ciudadanos. Los principios que deberán regir la política de protección de datos en el caso de la salud caso son los mismos a los que hacíamos mención con anterioridad, los de anonimización y del de seudonimización.

Respecto al principio de anonimización, tenemos el reciente ejemplo de lo sucedido, por ejemplo, con la herramienta que ha desarrollado el *Massachusetts Institute of Technology*, que ha puesto a disposición de las autoridades durante la pandemia una aplicación con técnicas de inteligencia artificial que permite distinguir a las personas asintomáticas infectadas por COVID19 a través de la simple grabación de sus toses<sup>180</sup>. La aplicación no identifica a la persona que tose, sino que únicamente usa sus datos para informarle de si esa tos pudiera implicar tener el virus. Se han usado los datos personales, pero nadie conoce ni puede conocer la identidad de la persona que cede su información a la aplicación. En este caso, al tratarse de datos anonimizados, no habría vulneración alguna del derecho a la privacidad.

De otro lado, la propia Unión Europea ha puesto de manifiesto recientemente la necesidad de que las autoridades públicas de los estados miembros incluyan el principio de seudonimización en el tratamiento masivo de datos

---

179 PIÑAR, J.L. Privacidad en estado de alarma y normal aplicación de la Ley [Blog]. (2020) accesible en <https://hayderecho.expansion.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/>

180 La inteligencia artificial detecta infecciones asintomáticas de Covid-19 a través de toses grabadas en el móvil. *La Vanguardia*. 2020, accesible en <https://www.lavanguardia.com/tecnologia/20201102/49165755736/inteligencia-artificial-detecta-infecciones-intomaticas-covid19-toses-movil.html>

en la lucha contra el COVID19.<sup>181</sup> Tanto es así que la herramienta aprobada por el Gobierno de España para la lucha contra el COVID19, basada en tecnología de inteligencia artificial, incluían la seudonimización como uno de los principios que tenía que regir el tratamiento de los datos personales. La cláusula décima de la Resolución de 30 de abril de 2020 para la operación de la Aplicación *ASISTENCIACOV19* en el contexto de la situación de crisis sanitaria ocasionada por el COVID-19, señala que “*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas que conozca y/o le sean informados efectivamente por el Responsable del Tratamiento el Encargado y Subencargado del Tratamiento aplicarán en función del análisis realizado conjuntamente con el Responsable del Tratamiento las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya: a) La seudonimización y el cifrado de datos personales...*”<sup>182</sup>

No se trata de una novedad, puesto que la Ley 41/2002 reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica ya recogía un sistema de seudonimización, si bien no llegaba a definir como tal este principio ni se estaba pensando entonces en el uso de la inteligencia artificial como es ahora el caso. La mencionada Ley, en su artículo 16.3, establece que “*el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*”

---

181 De este modo, en el considerando 25 de la Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados, señala que “*de acuerdo con el principio de minimización de datos, las autoridades públicas sanitarias y las instituciones públicas de investigación en el ámbito de la salud deben tratar únicamente los datos personales que sean adecuados y pertinentes, limitándose a lo necesario, y hacerlo con las debidas garantías, aplicando medidas como la seudonimización, la agregación, el cifrado o la descentralización.*”

182 BOE núm. 125, de 5 de mayo de 2020



## CAPÍTULO IV

### INTELIGENCIA ARTIFICIAL, ROBOTS Y RESPONSABILIDAD CIVIL

#### 1. LA RESPONSABILIDAD CIVIL EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL

No cabe duda de que uno de los puntos que suele generar más debate en torno a las nuevas tecnologías que han ido surgiendo a lo largo de la historia es el relativo a los posibles daños que estas pueden provocar. De este modo, cuestiones como la reparación de los daños producidos, las nuevas coberturas de los seguros o el sistema de responsabilidad civil aplicable, son una constante cada vez que se produce un cambio relevante en las técnicas, ya sean industriales o simplemente tecnológicas. Es lo que BECK denominó la sociedad del riesgo: en la modernidad avanzada, la producción social de riqueza va acompañada sistemáticamente por la producción social de riesgos<sup>183</sup>. Así, a lo largo del Siglo XIX y como “*hija de la mayor mecanización e industrialización*” que decía NAVARRETE, se desarrolló la conocida como responsabilidad civil por riesgo<sup>184</sup>, de la que, aunque luego analizaré con mayor detalle su contenido, sí conviene ahora señalar que su fin último era asegurar la reparación de los daños producidos por actividades peligrosas, en la mayoría de las ocasiones nuevas técnicas, por parte de quien las llevaba a cabo. Hoy, esas actividades que en ocasiones podríamos denominar incluso de consecuencias desconocidas, no son la mecanización o los vuelos, sino el uso de la inteligencia artificial o el internet de las cosas en distintos procesos, muchos de ellos cotidianos.

Asimismo, y como es lógico, de este debate no se ha quedado fuera la aplicación generalizada de procesos de inteligencia artificial. Tanto es así que la Comisión Europea creó en el año 2018 un grupo de expertos en res-

---

183 Vid. BECK, U.: *La sociedad del riesgo. Hacia una nueva modernidad*. Ed. Paidós. Barcelona. 1998.

184 Vid. NAVARRETE B, J.: “El origen de la responsabilidad civil objetiva en el derecho aéreo”, en *Revista Chilena de Derecho*, núm. 1, 1978, pág. 161

ponsabilidad y nuevas tecnologías para analizar la posible modificación, como luego se ha propuesto, de la legislación comunitaria en materia de responsabilidad civil en este ámbito<sup>185</sup>. Uno de los elementos que impulsó la creación de este grupo de expertos y la posterior propuesta de modificación de la Directiva 85/374 sobre responsabilidad por productos defectuosos fue precisamente el reto generado en nuestros días por la Inteligencia Artificial<sup>186</sup>. La propuesta, que ya ha pasado tanto por la Comisión Europea como por el Parlamento Europeo, propone la transformación de la Directiva en Reglamento, así como una armonización a nivel europeo del sistema de responsabilidad civil, modificando el concepto de productor, ampliando el de defecto y estableciendo un sistema de responsabilidad objetiva para los operadores en estos casos de actividades peligrosas. Posteriormente analizaré con detenimiento la mencionada propuesta, estableciendo un marco claro en lo relativo al sistema de responsabilidad civil para cada uno de los posibles implicados en los daños producidos por el uso de la inteligencia artificial. Son nuevos retos, algunos de ellos aun desconocidos, que pueden generar daños de muy diversos tipos. Los daños patrimoniales, corporales o morales seguirán existiendo, pero se producirán de una manera muy distinta, ante lo que el legislador debe de establecer unas normas nuevas que permitan, por un lado, el desarrollo de la inteligencia artificial y, por otro, la protección ante los posibles daños que esta pueda causar. Un equilibrio que, si bien puede resultar complejo, es del todo necesario.

En el año 2018 se produjo el primer atropello mortal por parte de un vehículo autónomo, cuyas decisiones y manejo se llevaban a cabo a través de un sistema de inteligencia artificial. Concretamente sucedió el 19 de marzo de 2018, cuando el sistema de un vehículo de Uber, según informó la propia compañía, fue incapaz de reconocer la existencia de un camión debido a la luz que daba directamente en el cristal<sup>187</sup>. Días después, y según las informaciones periodistas publicadas sobre el suceso, se produjo un nuevo accidente mortal, en esta ocasión el coche pertenecía a una de las compañías con mayor valor actualmente en bolsa, Tesla. Según la citada compañía, el

---

185 Dicha convocatoria fue publicada en el DOCE el 9 de marzo de 2018. Con fecha de 24 de mayo de ese mismo año me fue comunicado por la Comisión Europea mi inclusión, como suplente, en el mencionado grupo de expertos, lo que me ha permitido estar al día, no solo de los documentos públicos de la reforma, sino de todos aquellos internos

186 Así se recoge en el apartado 1.1.a de la convocatoria del Comité de expertos en responsabilidad y nuevas tecnologías, cuyo objetivo era el de “*proporcionar a la Comisión conocimientos especializados sobre la aplicabilidad de la Directiva sobre responsabilidad por productos defectuosos a los productos tradicionales, las nuevas tecnologías y los nuevos desafíos de la sociedad (formación de la Directiva sobre responsabilidad por productos defectuosos) y ayudar a la Comisión a elaborar principios que puedan servir de directrices para posibles adaptaciones de las leyes aplicables a nivel de la UE y nacional en relación con las nuevas tecnologías (formación de las nuevas tecnologías).*”

187 Vid. “Peligro al volante: por qué Tesla tiene tanta culpa como el conductor si hay un accidente”, *El Confidencial*, 2018, accesible en [https://www.elconfidencial.com/tecnologia/2016-07-02/tesla-piloto-automatico-coche-autonomo-muerte\\_1226761/](https://www.elconfidencial.com/tecnologia/2016-07-02/tesla-piloto-automatico-coche-autonomo-muerte_1226761/)

vehículo tenía activado el sistema automático de conducción y no fue capaz de evitar el accidente que, de otra manera, podría no haberse producido<sup>188</sup>.

Estos casos son solo un ejemplo de los daños producidos por vehículos autónomos pero que, por desgracia, no han sido los únicos en el sector de la inteligencia artificial en los últimos años, y lo serán aún menos en el futuro, por lo que a ello hay que darle una respuesta. Es cierto que el daño que puede provocar el atropello por parte de un vehículo tripulado será similar al producido por un vehículo dotado de inteligencia artificial que carezca de conductor, pero ¿debe de ser el sistema de responsabilidad civil el mismo? Con este ejemplo es sencillo concluir que, en el primer caso, en la gran mayoría de ocasiones, la responsabilidad que deberá aplicarse no será tanto al fabricante del vehículo, sino al conductor de este. En cambio, en el caso de un vehículo autónomo, la legislación aplicable deberá tener en cuenta no solo al conductor, operador como lo llama la propuesta realizada por la Comisión Europea, sino que tendrá que incluir, ante la posible concurrencia de responsabilidad civil, la del fabricante del vehículo además de la del programador o del desarrollador del software de inteligencia artificial. Para ello contaremos con dos vías, la responsabilidad extracontractual, que podrá ser la utilizada por aquel que sufre el daño, y la relativa a los daños por productos defectuosos que podrá ser la vía elegida tanto por el que sufre el daño como por aquél responsable del mismo que pretenda repetir la responsabilidad con el resto de los actores. La concurrencia de responsabilidad, como más tarde veremos, se convertirá en un elemento esencial en esta materia y que tendrá que ser tenida muy en cuenta por el legislador. Sucede que esta última legislación, la relativa a la responsabilidad por productos defectuosos, deriva de una directiva europea de mediados de los años ochenta, cuya modificación, como ya hemos señalado y sobre la que más tarde ahondaremos, se hace hoy absolutamente necesaria.

Son muchos los ejemplos que podríamos poner en los ámbitos más diversos, algunos de los cuales hemos ya mencionado en el primer capítulo del presente libro. Desde la toma de una decisión injusta y dañina en base a la propuesta realizada por la inteligencia artificial, a una aplicación que cuente también con un algoritmo que provoque cualquier tipo de daño sea físico o no. Piensen, por ejemplo, en una aplicación para la compra de acciones bursátiles que, basada en inteligencia artificial, provoque graves pérdidas en sus usuarios. Esto fue lo que sucedió el 6 de mayo de 2010 cuando se produjo una de las mayores caídas de la bolsa de Wall Street. El índice Dow Jones cayó en unos segundos más del 10%. Una de las compañías que operaba grandes cantidades de dinero ese día estrenó un nuevo programa basado en inteligencia artificial que cometió el error de efectuar una venta masiva a

---

188 Vid. "Tesla reconoce un nuevo accidente mortal por un coche autónomo." *La Vanguardia*, 2018, accesible en <https://www.lavanguardia.com/tecnologia/20180331/442086876630/tesla-muerte-conduccion-autonoma.html>

largo plazo en contratos de 20 minutos<sup>189</sup>. También podríamos pensar en el daño que generaría la designación de uno u otro candidato para un puesto de trabajo habiendo usado un algoritmo discriminatorio con las mujeres o con los discapacitados.

Las preguntas a las que tendremos que dar respuesta serán: ¿Quién es el responsable de que se haya tomado esa decisión? Y, a su vez, ¿Ha sido esa decisión la única culpable del daño causado o han intervenido otros factores? Piensen, por ejemplo, en una decisión que, aun pudiendo ser acertada, sea mal ejecutada, bien por defecto de fabricación de la máquina que tiene que llevarla a cabo, bien por un negligente cuidado o mantenimiento del hardware o bien por la negligencia o impericia de la persona que debiere ponerla en marcha.

Una parte de la doctrina sostiene que la persona física o jurídica titular del robot debería ser el criterio utilizado para determinar quién es el responsable de los daños producidos éstos. Se refiere, en este caso, como titular del producto al fabricante<sup>190</sup>. Sin duda, el propietario o el operador deberán asumir los riesgos que genera el uso de esta tecnología, en los términos adecuados como ahora explicaré. Aunque luego me detendré en ello, una de las propuestas que realiza la Comisión Europea para ello es exigir al propietario la contratación de un seguro de responsabilidad civil obligatorio para poder afrontar los daños causados por aquello de lo que es titular. También parece lógico que el encargado de supervisar o utilizar el software o hardware tenga que contar con una formación determinada. Habrá que estudiar también el papel del desarrollador del software basado en inteligencia artificial, como posteriormente haremos. Respecto a este último he de señalar que, frente a lo que sucede con el operador, presentará ciertas dificultades hacerlo objetivamente responsable del daño, entre otras cosas porque puede que la causa del daño no provenga del diseño de ese software, sino en la aplicación de este o de cualquier otra circunstancia ajena. Es ahí donde la relación de causalidad, que también estudiaremos con profundidad, jugará un papel fundamental. Prestaré también especial atención a un sujeto clave, el fabricante o productor del robot o la aplicación concreta. Todo ello lo analizaré posteriormente de forma pormenorizada.

Pasaré a continuación a estudiar diversas cuestiones de interés relacionadas con la responsabilidad civil en este ámbito. Comenzaré con el estudio relativo a la posibilidad de que los robots pudieran ser responsables de los

---

189 . Vid. “Las causas del flash crash al descubierto: La SEC publica su informe oficial”, *El Economista*, 2010. Accesible en <https://www.eleconomista.es/mercados-cotizaciones/noticias/2492339/10/10/Las-causas-del-flash-crash-al-descubierto-la-SEC-publica-su-informe-oficial.html>

190 Vid. PLAZA PENADÉS, J.: “Aspectos legales de la Inteligencia Artificial y el Big Data”, *Big Data e Inteligencia Artificial. Una visión económica y legal de estas herramientas disruptivas*, Ed. Universidad de Valencia, 2018, pág. 40

daños cometidos por ellos mismos, para luego pasar al análisis de la actual Directiva 85/374 relativa a la responsabilidad civil por productos defectuosos, finalizando con el análisis crítico sobre la propuesta de modificación legislativa en este ámbito efectuada por las instituciones europeas.

## **2. ¿PUEDEN LOS ROBOTS SER CIVILMENTE RESPONSABLES DE LOS DAÑOS OCASIONADOS POR ELLOS?**

Como ahora veremos, una de las circunstancias que complican de forma decisiva las reglas de responsabilidad civil en el ámbito de la inteligencia artificial será la participación, en la mayoría de las ocasiones, de muchos y diversos actores. Entre ellos podemos señalar, al menos, el diseñador del algoritmo, el encargado de proporcionar los datos en los que este se base, el fabricante del producto, el propietario de este, o el responsable de su uso, manejo o supervisión, denominado por la propuesta de la Comisión Europea como operador. Todos ellos podrán participar, de una manera o de otra, en la causación del daño. A esto debemos añadirle la participación directa del propio hardware -robot-, al que algunos autores, como ya hemos visto someramente, pretenden hacer responsable directo de esos daños producidos.

He venido señalando a lo largo de todo el trabajo que uno de los elementos que distinguen a la inteligencia artificial es la capacidad de tomar decisiones con autonomía o de aprender del entorno sin la necesidad de intervención del ser humano. Es cierto que la legislación va en la línea de exigir la participación del ser humano, bien en la misma decisión, bien en el control de esta. Es precisamente este motivo el que hace fundamental estudiar en profundidad los criterios de imputación de la responsabilidad civil para tener en cuenta quién habrá de responder por los daños causados.

Analizaré ahora distintas cuestiones que se plantean sobre la imputación del daño, centrándonos en la posibilidad de que pueda imputársele este al verdadero causante de este, en sentido material, que será el robot o incluso el software. Y lo haré volviendo sobre una de las cuestiones ya tratadas anteriormente, la existencia de personalidad o no en los robots. Una cosa es evidente, sin personalidad no habrá responsabilidad posible que imputar. Como ahora trataré de hacer ver, la resolución de estas cuestiones será técnicamente compleja porque, aunque a primera vista pudiera parecer lógico para cualquier observador ajeno al ámbito del Derecho que fuese responsable el propietario o el usuario del robot como sucede en el caso de los vehículos tradicionales, no podemos olvidar a todos los participantes en el proceso de fabricación de los mismos.

Respecto a la cuestión que había planteado al inicio de este epígrafe, la de si el robot pudiera ser responsable del daño causado, debemos descartarlo. Parto de la premisa de que los robots, como ya hemos mencionado, son objetos, y como tales deberán ser analizados como productos a efectos del

estudio de la responsabilidad civil. Así pues, los robots no tienen personalidad jurídica y no pueden ser, de forma alguna, titulares de derechos o de obligaciones. Ha sido el propio comité de expertos de la Comisión Europea el que ha reiterado que, “*a efectos de responsabilidad, no es necesario dotar de personalidad jurídica a los sistemas autónomos*”<sup>191</sup>.

Siempre, en cualquier caso, detrás de un robot, detrás de un algoritmo o de un software vamos a encontrar una persona, ya sea física o jurídica. El fabricante del producto, el ingeniero que diseñó la aplicación, el propietario del producto o el que maneja al robot. Entre ellos, y en la mayoría de las ocasiones concurrirán varios de los actores ahora mencionados, encontraremos al responsable del daño producido.

En definitiva, en ningún caso se le puede atribuir a una cosa la capacidad de responder de los daños provocados a terceros, puesto que estos solo pueden ser consecuencia última de la actuación, o incluso de la omisión, del ser humano.<sup>192</sup> Como afirma EBERS, cualquier acto de la inteligencia artificial siempre “*permanece enlazado a la acción humana, lo que es jurídicamente relevante y significa que, en última instancia, siempre se deja ver una persona imputable*”<sup>193</sup>.

Es cierto que, aunque no comparta su postura, no puedo obviar que una parte de la doctrina ha planteado la imputación de los robots como una solución al problema de la responsabilidad civil. Así, PALMIERI sostiene que “*la personalidad electrónica es considerada un enfoque plausible al problema de la responsabilidad, tanto para los robots dotados de un cuerpo como para los softwares robots que exhiben un cierto grado de autonomía e interactúan con las personas.*”<sup>194</sup> Se basa este autor en la autonomía que pueden llegar a tener los robots para hacerlos responsables de los daños. Pero, como afirma acertadamente DÍAZ ALABART, ese grado de autonomía no sería suficiente como para hacerles responsables de los daños, lo mismo que no se responsabiliza a los animales y sí a sus dueños, a pesar de que aquellos “*también aprenden, tienen esa cierta autonomía e impredecibilidad*”<sup>195</sup>.

---

191 Así se recoge en la recomendación 8 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 6

192 Vid. GÓMEZ LIGÜERRE, C., y GARCÍA-MILCÓ, G.: “Liability for Artificial Intelligence and other emerging technologies”, en *Revista para el análisis del Derecho*, núm. 1, 2020, pág. 501

193 Vid. EBERS, M. “La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?”, en *Indret Revista para el Análisis del Derecho*, núm. 3, 2016, pág. 8

194 Complementa esta afirmación el autor manteniendo que “*a esta propuesta se suma, naturalmente, la necesidad de crear un registro y dotar a cada robot de una identificación al momento de su puesta en el comercio, además de asegurar que le sea asociado un fondo a través del cual sea factible responder por las obligaciones.*” Vid. PALMIERI, E., “Robótica y derecho: sugerencias, confluencias, evoluciones ... Op. cit., pág. 78

195 Vid. DÍAZ ALABART, S.: “Robots y responsabilidad civil”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018, pág. 110

Es cierto que en el informe de 2017 del Parlamento Europeo, al que ya he hecho mención anteriormente, se planteaba ya entonces la posibilidad de que los robots pudieran considerarse “*personas electrónicas responsables de reparar los daños que puedan causar...*”, y lo hacía incluso cuestionándose si debía de ser una responsabilidad objetiva o, por el contrario, una responsabilidad basada en el riesgo.<sup>196</sup> Esta postura inicial de la institución europea ya ha sido corregida en informes más recientes que descartan la posibilidad de solucionar la cuestión de la responsabilidad civil mediante la atribución de personalidad a los robots<sup>197</sup>. Ya en un capítulo anterior argumenté someramente por qué debemos descartar esa opción. Me permito resumir nuevamente, a riesgo de ser reiterativo, los cuatro principales motivos por los que estoy convencido de que la imputación como tal de los robots carece de sentido y generaría muchos más problemas que soluciones.

El primero de ellos es que los robots, la inteligencia artificial, carecen de derechos y obligaciones y, por lo tanto, no tiene patrimonio alguno con el que responder ante los daños causados. Siendo la reparación del daño el principal elemento de la responsabilidad, me refiero en esta ocasión únicamente a la responsabilidad civil que no penal, esta devendría prácticamente imposible. Y ello a pesar de las más o menos imaginativas fórmulas ya mencionadas anteriormente de dotar de patrimonio a los robots a través de la reserva de un porcentaje de su producción económica. Como digo, algunos autores siguen manteniendo la posibilidad de que los robots sean los responsables directos de los daños que causen, incluso en el caso en el que carezcan de personalidad jurídica alguna, algo que se me antoja del todo inviable.

Traigo nuevamente al caso la postura ya comentada de ERCILLA, en la que no solo sostenía la necesidad de que los robots tuviesen algún tipo de personalidad jurídica, sino que reclamaba que pudiesen ser titulares de un patrimonio, precisamente para afrontar el resarcimiento de los daños que hubiesen podido provocar<sup>198</sup>. Recordamos que la propuesta se basaba en que los robots acumulasen un patrimonio a través de un porcentaje de lo que produjesen, una parte destinada al patrimonio del dueño del robot, y otro al robot mismo.

En la misma línea, GUNTHER sostiene que la posibilidad de dotar de personalidad jurídica a los robots estaría ligada a la responsabilidad civil de estos. Según este autor, a los robots se les dotaría de una serie de activos para que las personas que interactuasen con los robots pudieran conocer la cuan-

---

196 , Cfr. Parlamento Europeo (2017), *Informe con recomendaciones ... Op. cit.*, pág. 19 y 20

197 Vid. 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

198 Vid. ERCILLA GARCÍA, J.: “Aproximación a una Personalidad... Op. cit.”, pág. 6

tía por la que podrían responder por los daños que hubiesen provocado<sup>199</sup>. A este respecto, los expertos nombrados por la Comisión Europea para realizar el informe sobre responsabilidad civil e inteligencia artificial, también se han mostrado contrarios a la posibilidad de otorgar personalidad jurídica alguna a los robots. Señala el citado informe que “*en teoría, la personalidad jurídica podría consistir únicamente en obligaciones. Sin embargo, esta solución no sería útil en la práctica, ya que la responsabilidad civil es una responsabilidad patrimonial, que requiere que su portador tenga bienes. [...] Además, para dar una dimensión real a la responsabilidad, los agentes electrónicos podrían adquirir bienes por sí mismos. Esto requeriría la resolución de varios problemas legislativos relacionados con su capacidad jurídica y su forma de actuar al realizar transacciones legales*”<sup>200</sup>. Comparto plenamente la postura de los expertos. No solo no veo viable la propuesta sostenida por parte de la doctrina, sino que no encuentro las soluciones que esta puede aportar.

En este sentido, con la postura de parte de la doctrina se muestra también muy crítico ROGEL VIDE, llegando a afirmar que “*El siguiente paso –al margen de la aberración que entraña– es considerar a los robots como personas, como sujetos de derechos y hasta de obligaciones, responsables incluso de hipotéticos daños causados por ellos, y tal paso, más o menos tímidamente, tiende a darse, se ha dado no solo por científicos tan apasionados por la robótica como legos en Derecho, sino también, lo que es más preocupante, por legisladores expertos*”<sup>201</sup>. En el mismo sentido se ha manifestado PLAZA PENADÉS, mostrándose contrario a que los robots puedan tener personalidad jurídica alguna, descartando, por lo tanto, que éstos puedan “*tener responsabilidad propia, más allá de que no tengan patrimonio o capacidad patrimonial para hacer frente a dicha responsabilidad*”<sup>202</sup>.

El segundo de los motivos a los que antes me refería, y por el que entiendo que no se le tendría que imputar la responsabilidad a los robots, es que esta fórmula abriría la posibilidad a una circunstancia que considero peligrosa, que no es otra que la exención de responsabilidad del resto de agentes participantes en la acción que pudo provocar el daño. Es cierto que podría también existir un sistema de concurrencia de culpa, pero también lo es que, llegado el caso, podríamos encontrarnos con que el único que respondería bajo un sistema de responsabilidad civil objetiva sería el robot.

---

199 Para esta circunstancia proponen los autores que, aunque básicamente la reparación estaría cubierta por sus activos “*parece plausible que en ciertos casos la transferencia de este pago pueda emitirse a quienes participan en la creación o utilización de la máquina, especialmente en casos claros e identificables en que un mal funcionamiento específico de la máquina pueda atribuirse a una conducta gravemente negligente o dolosa*.” Vid. GUNTHER, J., MUNCH, F., BECK, LOFFLER, S. y LABRUTO, R.. “Issues of privacy and electronic... Op. cit., pág. 819

200 Informe del Comité de expertos sobre la responsabilidad civil en la inteligencia artificial y tecnologías emergentes, 2020, pág. 38

201 Vid. ROGEL VIDE, C.: “Robots y personas”, *Los robots...* Op. cit. págs. 16 y 17

202 Vid. PLAZA PENADÉS, J.: “Aspectos legales de la Inteligencia Artificial...”, Op. cit., pág. 41

Se convertiría, por lo tanto, en la vía más cómoda, directa y sencilla para la reclamación de cualquier perjudicado. A mayor abundamiento, el robot no tendría interés alguno en repetir la reparación con el resto de actores, lo que llevaría a la práctica impunidad de estos.

Una tercera causa por la que me opongo a la posibilidad de hacer responsables de los daños a los robots, aunque muy ligada al anterior motivo, es que esa supuesta responsabilidad eliminaría uno de los elementos colaterales, aunque no se trataría del principal de la responsabilidad civil, como es la intención de prevenir el daño. Como señala TENA, “*la reparación del daño puede cumplir por sí sola funciones de disuasión que colman los fines de prevención particular de rehabilitación y general de disuasión típicos del Derecho penal*”<sup>203</sup>. La propia Comisión Europea, en su reciente informe sobre responsabilidad civil en la inteligencia artificial, ya mencionado, ha puesto de manifiesto este elemento del que hablo, afirmando que las normas de responsabilidad civil también “*proporcionan incentivos económicos a la parte responsable para que no cause dicho perjuicio*”<sup>204</sup>.

La última de las razones por las que me opongo a esta supuesta solución es precisamente porque esta propuesta de atribuir la responsabilidad civil a los robots o sistemas generaría un problema de legitimidad, pues los robots no tendrían capacidad procesal para poder ser demandados y formar parte de un proceso judicial. Por mucho que un robot estuviese diseñado para realizar una determinada tarea o función con un alto grado de especialización, eso no significa que fuese capaz de comprender un procedimiento jurídico, de elegir un abogado o una línea de defensa o de comprender lo que se le reclama. En último caso, sería el dueño del robot el que tendría que asumir esa defensa, o el productor de este, pero ello carecería de sentido en un sistema como el nuestro.

Algunos autores han llegado a proponer que pudiera resolverse de manera similar a como se hacía en la antigua Roma con los daños generados por los esclavos, esto es, demandando al dueño del mismo, incorporando la acción pretoria, por la que éste solo respondería por el importe del *peculio*<sup>205</sup>. Me cuesta llegar a imaginar una demanda de responsabilidad civil dirigida contra un robot, y no tanto si fuese dirigida contra el dueño del mismo, el productor o el operador.

En definitiva, los robots no responderán de los daños provocados, como no reciben remuneración por su actividad, ni tienen días de vacaciones. Los robots no son personas, ni jurídicas ni físicas, sino cosas. Así pues, como tales deberán ser tratadas también en el ámbito de la responsabilidad civil.

---

203 Vid. TENA R.: “Hacia un salto evolutivo en el Derecho civil... Op. cit.

204 Vid. Comisión Europea, *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*, 2020

205 Cfr. ERCILLA GARCÍA, J.: “Aproximación a una Personalidad... Op. cit., págs.. 6 y 7

### 3. SISTEMA DE RESPONSABILIDAD CIVIL POR LOS DAÑOS PRODUCIDOS COMO CONSECUENCIA DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Debemos partir de que el objetivo de establecer una normativa en esta materia sobre responsabilidad civil no es otro que el de garantizar que tanto los productos como los servicios dotados con inteligencia artificial sean, por un lado, lo más seguros posibles y, por otro, garanticen la reparación de los daños que puedan llegar a producirse por el uso de esta técnica. Como acertadamente ha señalado la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, “*la legislación debe establecer normas claras y equilibrar las obligaciones para proteger a ambas partes en un contrato y a los terceros que necesitan certidumbre sobre el ámbito en el que solicitar reparación por daños y perjuicios*”<sup>206</sup>.

Tanto la propuesta de los expertos como las recomendaciones de la Comisión Europea y del Parlamento Europeo hacen hincapié en la necesidad de adaptar las leyes nacionales para convertir la responsabilidad objetiva, en el caso de los operadores, o por riesgo, en el sistema que rija en totalidad de los países de la Unión Europea en todo lo que tenga que ver con los daños provocados por la inteligencia artificial. Como ya he señalado, España cuenta desde hace décadas con una legislación que prevé un sistema de responsabilidad cuasi objetiva o por riesgo, por lo que la posible modificación legislativa se tendría que limitar a los aspectos sobre los que ahora me detendré como la definición de producto y productor, la ampliación del concepto de defecto y la inclusión de un sistema de responsabilidad absolutamente objetivo para el operador, figura clave en la propuesta de Reglamento europeo. Todo ello pasa, en cualquier caso, por la limitación de las causas de exoneración de responsabilidad actualmente existentes, así como por el establecimiento de un sistema de responsabilidad específico y objetivo en muchos casos para el operador, un sujeto que, aun pudiendo en ocasiones ser el mismo que el productor, será la piedra angular en la que pivote la reforma. Se ha de tener en cuenta también que la propuesta de las instituciones europeas pasa por la aprobación del Reglamento ahora mencionado, por lo que este sería de aplicación directa en nuestro país sin necesidad de modificación legislativa alguna.

El informe de los expertos ya referido establece la conveniencia de contar con un régimen de responsabilidad civil basado en el riesgo, incluso objetiva en según qué casos, para garantizar que siempre que se produzca un daño la víctima pueda ser indemnizada independientemente de la existencia de culpa o no. Aunque esta conclusión es matizada posteriormente en dos aspectos. El primero, el referido a la necesidad de determinar de manera ponderada quién es el que ha de ser el responsable civil. Como luego veremos la novedad incorporada pasa por la inclusión de la figura del operador. El

---

<sup>206</sup> Cfr. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (2018), *Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial*, pág. 3

segundo, volviendo sobre algo de lo que ya he hablado, la necesidad de que el enfoque se lleve a cabo teniendo en cuenta el riesgo que la puesta en circulación del producto pueda conllevar. Como ya he venido señalando, son varios los agentes que podrán tener relación con los posibles daños causados por sistemas o robots que se encuentren diseñados o contengan inteligencia artificial, en los que ahora me detendré.

Tanto la doctrina como las instituciones europeas no han dudado en señalar que el régimen de responsabilidad civil, en lo que a la inteligencia artificial se refiere, actualmente pasa por lo establecido en la Directiva del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, en adelante Directiva 85/374. Pero también es cierto que el Parlamento Europeo y la Comisión Europea han señalado la necesidad de modificar la mencionada directiva, y en la aprobación de un nuevo Reglamento Europeo que permita la adaptación a la nueva realidad, incluyendo, como no puede ser de otra manera, las novedades aportadas por la inteligencia artificial.

Anteriormente puse de manifiesto la creación por parte de la Comisión Europea en el año 2018 de un grupo un Grupo de Expertos sobre responsabilidad y nuevas tecnologías cuyo resultado ya fue trasladado al Parlamento Europeo en forma de una propuesta que incluye la modificación de la citada directiva. Dicha modificación no será una modificación radical de la actual Directiva 85/374, sino que se tratará de “*algunos ajustes necesarios*”, ante la aparición de nuevas técnicas<sup>207</sup>. A esta propuesta me referiré con detenimiento a lo largo del presente capítulo, prestando especial atención a las modificaciones más significativas, no sólo en el régimen de responsabilidad civil aplicable, sino también en la necesaria modificación y ampliación de alguno de los conceptos tradicionales incluidos en ella como son los de producto, defecto o daño.

También el Parlamento Europeo ha elaborado una serie de recomendaciones para la elaboración de un Reglamento europeo y del Consejo relativo a la responsabilidad civil por el Funcionamiento de los Sistemas de inteligencia artificial. Considera esta institución europea que, a pesar de que la Directiva 85/374 “*ha demostrado ser durante más de treinta años un medio eficaz para obtener una indemnización por un daño causado por un producto defectuoso... debe revisarse para adaptarla al mundo digital y abordar los retos que plantean las tecnologías digitales emergentes*”<sup>208</sup>. La mencionada propuesta, como ya he mencionado, pasa por aprobar un Reglamento Europeo que sea capaz de adap-

---

207 Vid. Parlamento Europeo (2020), *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*, pág. 14

208 Informe del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)), introducción núm. 8, pág. 7

tar algunos conceptos que han quedado ya anticuados y permita también homogeneizar los sistemas de responsabilidad civil en toda la Unión Europea. La propuesta, que pasó previamente por el comité de asuntos jurídicos del Parlamento Europeo, consta de veinticuatro considerandos, quince artículos y un anexo. Es importante resaltar que se apuesta por un Reglamento, y no por una Directiva, con el objetivo de conseguir una armonización real, absoluta e inmediata respecto a los aspectos fundamentales en materia de responsabilidad civil por los daños causados por la inteligencia artificial.

Además de la propuesta sobre el Reglamento Europeo de responsabilidad civil al que me vengo refiriendo, haré mención de la recientemente publicada propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican determinados actos legislativos de la Unión. En esta última se clasifican los sistemas de inteligencia artificial en tres categorías; los sistemas prohibidos, los de alto riesgo, y aquellos que no están ni prohibidos ni son de alto riesgo. Ello será fundamental a la hora de establecer el sistema de responsabilidad civil para los operadores, que en los dos primeros casos será objetivo, mientras que en el último tendrá carácter subjetivo.

Intentaré analizar a lo largo del siguiente apartado tanto el sistema actual de responsabilidad civil, en vigor aun, como la nueva propuesta de Reglamento que, en un futuro no lejano, se convertirá en la herramienta básica para la reparación de los daños causados por la inteligencia artificial.

### **3.1. El régimen de responsabilidad civil aplicable actualmente: La Directiva 85/374 y los daños provocados por la inteligencia artificial.**

Como ya he señalado, el sistema de responsabilidad civil instaurado actualmente en Europa pasa por el establecido en la Directiva 85/374, concretado en nuestro país por el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Ambas legislaciones han sido eficaces respecto a los objetivos que se habían planteado, aunque, llegado este punto, han de ser revisadas debido a que la aparición de nuevas técnicas ha superado alguno de sus postulados como ahora pondré de manifiesto.

Es comúnmente aceptado que cuando una actividad, ya sea empresarial o profesional, genere unos determinados beneficios y simultáneamente sea una potencial amenaza para las personas o sus bienes, aquellas deben asumir la reparación de los daños provocados. Esa fue la filosofía que inspiró la legislación europea en materia de protección a los consumidores y relativa a la responsabilidad por productos defectuosos. En nuestro país, la primera norma que trató este aspecto fue la Ley General para la Defensa de los Con-

sumidores y Usuarios, de 19 de julio de 1984. Pero la verdadera revolución fue introducida por la Unión Europea a través de la Directiva 85/374/CEE, de 25 de julio relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, de la que ahora hablaremos con detenimiento. Ya años más tarde, España promulgó la Ley 22/1994, de 6 de julio como transposición de la mencionada directiva, y que fue reemplazada por el hoy vigente Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias que continúa hoy en vigor.

El proceso de formación de la Directiva 85/374 fue largo y complejo que, finalmente, tras un largo e intenso debate, dio sus frutos el 25 de julio de 1985 con la aprobación de esta. La problemática más importante se encontraba en dos puntos polémicos como eran el establecimiento de un tope máximo en la indemnización por los daños producidos, que aún hoy sigue generando un importante debate, y la posible incorporación o no de los riesgos al desarrollo.

Una de las normativas que mayor influencia tuvo en la Directiva 85/374 fue el Convenio europeo sobre la responsabilidad derivada de los productos en caso de lesiones corporales o de muerte, que data del año 1977 y en el que se consagraba por vez primera en Europa el principio de responsabilidad objetiva<sup>209</sup>. Desde entonces, incluso ahora en la nueva propuesta realizada por la Comisión Europea, la responsabilidad objetiva ha estado presente con mayores o menores matices; con más o menos exenciones de responsabilidad.

Por lo que respecta al contenido de la Directiva 85/374, hay que señalar que incluía los dos objetivos que se habían planteado como prioritarios; por una parte, la protección y tutela de los consumidores europeos, no solo de su salud y seguridad sino también de sus intereses económicos. De este modo se consideran indemnizables, según lo establecido en el artículo 9 de la Directiva 85/374, los daños causados por muerte o lesiones corporales, los daños causados a una cosa o la destrucción de una cosa, que no sea el propio producto defectuoso con la condición de que tal cosa sea de las que normalmente se destinan al uso o consumo privados y el perjudicado la haya utilizado principalmente para su uso o consumo privados. Por otro, el establecimiento de un sistema único de responsabilidad civil para todos los productores de los distintos Estados miembros. Pero, a pesar de este intento por lograr la armonización, el Tribunal de Justicia de la Unión Europea ha señalado en varias ocasiones que los Estados miembros gozan de cierta libertad para establecer regímenes de responsabilidad diversos al de la objetiva

---

209 RODRÍGUEZ CARRIÓN, J. L.: *La responsabilidad civil por los daños causados por productos defectuosos*. Ediciones Revista General de Derecho. Valencia, 2000. Pág. 19

que rige en la Directiva<sup>210</sup>. Es evidente que el no haber conseguido definitivamente esta armonización ha provocado una desigualdad entre los productores evidente, especialmente en lo que respecta al establecimiento de un sistema de responsabilidad subjetivo frente a otro objetivo, teniendo unos productores que soportar una mayor carga económica que otros<sup>211</sup>.

Lo que realmente me ocupa en este trabajo es el sistema de responsabilidad civil instaurado en la Directiva y que afecta directamente a los daños que pueden ser provocados por la inteligencia artificial. Con carácter general, podemos afirmar que se trata de un régimen de responsabilidad cuasi objetiva o sin culpa, por el que el perjudicado tan solo tendría que probar la existencia de defecto en el producto, el daño que se hubiese producido y el nexo de causalidad entre ellos. Concretamente, el artículo 4 de la Directiva afirma que “*el perjudicado deberá probar el daño, el defecto y la relación causal entre el defecto y el daño.*” Así pues, deja al lado la obligación de probar la culpa, elemento este que caracteriza a la responsabilidad subjetiva.

Este principio, el de la responsabilidad cuasiojetiva, se mantiene en todos sus términos en la propuesta vigente de modificación de la Directiva. Como posteriormente trataré de acreditar, una de las novedades más destacadas en este sentido es la exclusión de alguna de las causas de exoneración de la responsabilidad civil existentes actualmente y que se pretende que desaparezcan. Otros aspectos a destacar, además del establecimiento de ese régimen de responsabilidad cuasi objetiva para fabricante del producto, son los relativos a la valoración más objetivada del concepto de defecto, el establecimiento de acciones propias en beneficio del perjudicado y el nacimiento de la obligación por parte del fabricante de suscribir un seguro de responsabilidad civil.

Así pues, en la legislación actual, aplicable a los daños producidos por productos defectuosos, nos encontramos con un sistema de responsabilidad prácticamente objetiva, frente al tradicional de responsabilidad subjetiva, que se basaba en la afirmación de que no hay responsabilidad sin culpa.

Es cierto que existió cierto debate entre la doctrina acerca de si hay una diferencia significativa entre la responsabilidad por riesgo y la objetiva. Ambos sistemas se caracterizan indudablemente por no ser la culpa el fundamento del criterio de imputación de la responsabilidad. Comparto la postura de RODRÍGUEZ LLAMAS cuando sostiene que la diferencia reside en que para el nacimiento de la obligación de resarcir en un sistema de responsabilidad objetiva ha de mediar una relación de causa-efecto y por lo tanto, serían causas de exoneración de responsabilidad objetiva aquellas que descansen en la ruptura del nexo causal; En cambio, en el caso de responsabili-

---

210 Sentencia de 10 de enero de 2006, del Tribunal de Justicia de la Unión Europea, asunto *Skov c/ Bilka Lavarishvareus*

211 . RODRÍGUEZ LLAMAS, S.: *Régimen de Responsabilidad Civil por Productos Defectuosos...* cit. Pág. 58.

dad por riesgo podrá exonerarse de responsabilidad, no solo en aquellos casos en que se produzca la ruptura del nexo causal, sino también en aquellos casos en los que no concurra el riesgo típico delimitado por la legislación<sup>212</sup>.

En el Texto refundido, al igual que en la Directiva, se establecen en el artículo 140 una serie de causas de exoneración, a pesar de las cuales podemos señalar que se basa igualmente en un régimen de responsabilidad objetiva, aunque en algunos casos, los que no afecten al operador, ni absoluta ni plena, o, como define JIMÉNEZ LIÉBANA, una responsabilidad objetiva limitada, originada por la puesta en circulación de productos defectuosos<sup>213</sup>.

### **3.2. El régimen de responsabilidad civil en la futura legislación europea sobre inteligencia artificial**

Dicho lo anterior, no cabe duda de que la evolución de las nuevas tecnologías, especialmente las relacionadas con la inteligencia artificial, hace que nos planteemos la necesidad de modificar la legislación existente para dotar de mayor seguridad a los ciudadanos europeos. La comisión de expertos impulsada por la Comisión Europea ha concluido en el ya mencionado informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, que esa modificación debe llevarse a cabo sin mayor demora, y ello en base a que las características de estas nuevas técnicas “*ponen en entredicho aspectos de los marcos de responsabilidad civil nacionales y de la Unión y podrían menoscabar su eficacia.*” El principal riesgo que encuentra la Comisión Europea es el relativo a la dificultad que puede conllevar “*la determinación de la relación causal entre los daños producidos y un comportamiento humano.*” Efectivamente, el daño directo lo realizará ese sistema de inteligencia artificial, ya sea de forma material o inmaterial, pero hemos de ser capaces de determinar qué comportamiento humano fue el que lo provocó. Puede que sea un diseño erróneo del software, una actualización inadecuada o un uso inconveniente, por señalar algunas posibilidades, pero siempre, en cualquier caso, existirá un nexo con la actividad de una persona física o jurídica.

Entrando ya en lo que al sistema de responsabilidad civil se refiere, dice textualmente el informe que debe plantearse “*sobre la base de un enfoque específico basado en el riesgo.*” No cabe duda de que, si en circunstancias normales no siempre es fácil determinar la culpabilidad en el daño causado, mucho más difícil lo será si ese daño se produce con la participación de tecnologías como la inteligencia artificial.

Como ahora trataré de explicar, distingo la propuesta definitiva entre el sistema de responsabilidad civil necesario para los operadores y el del resto

---

212 RODRÍGUEZ LLAMAS, S.: *Régimen de Responsabilidad Civil por Productos Defectuosos...* cit. Págs. 37 y ss.

213 Vid. JIMÉNEZ LIÉBANA, D.: *Responsabilidad civil: daños causados...* cit. Pág. 112

de los actores. Los primeros incluyen, según la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo denominada Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial, al proveedor, al usuario, al representante autorizado, al importador y al distribuidor<sup>214</sup>. De este modo, en el caso de los operadores las instituciones europeas se inclinan por un sistema absolutamente objetivo para aquellas actividades en las que el sistema de inteligencia artificial sea considerado peligroso o de alto riesgo, mientras que para aquellos que no lo sean se manifiesta favorable a diseñar un sistema de responsabilidad subjetivo. Esto, como señala parte de la doctrina, puede conllevar un problema, que no es otro que el perjudicado decida reclamar única y exclusivamente al operador, y que sea este el encargado, en su caso, de repetir frente al resto de posibles responsables como los productores o programadores, aunque estos. De este modo, EBERS se inclina porque la futura legislación relativa a los daños producidos por la inteligencia artificial pase por un sistema de responsabilidad por riesgo en el que tanto productor como operador respondan del daño causado como obligados solidarios<sup>215</sup>.

La propuesta no aboga por la generalización de la responsabilidad objetiva, sino que pasa porque la responsabilidad del productor esté basada en el riesgo, como actualmente se recoge ya en la Directiva 85/374. Como señalan GÓMEZ LIGÜERRE y GARCÍA-MILCÓ, “*no todos los daños imaginables serán causados por defectos del dispositivo y el Informe es cauto a la hora de extender la responsabilidad objetiva a supuestos en los que la responsabilidad del fabricante no sea de aplicación*”<sup>216</sup>.

No debemos obviar que la propuesta de Reglamento establece en su artículo 11 una responsabilidad solidaria para el caso en el que haya más de un operador del sistema de inteligencia artificial. Prevé también el caso en el que tan solo exista un operador y que este sea a su vez el productor del sistema, en cuyo caso el sistema de responsabilidad civil que prevalecerá será

---

214 Art. 3.8de la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo denominada Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial

215 El autor advierte de que el establecimiento de una responsabilidad por riesgo para el dueño del producto “*podría llevar a proceder unilateralmente contra el operador. No sólo se dirigirían los perjudicados por razones objetivas y de cercanía local antes al operador que al productor. También podría perfectamente ocurrir que una responsabilidad del operador, concebida como responsabilidad por riesgo, fuese más atractiva que la responsabilidad del productor, ya que esta, en la Directiva, no ha sido diseñada como una responsabilidad por riesgo pura, sino como un sistema de responsabilidad mixto, con elementos estrictos y basados en la culpa.*” Vid. EBERS, M.: “La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?”, en *Revista para el análisis del Derecho*, núm. 3, 2016, págs. 15 y 16

216 Vid. GÓMEZ LIGÜERRE, C., y GARCÍA-MILCÓ, G.: “Liability for Artificial ... Op. cit., pág. 505

el del futuro Reglamento que, recuerdo, es más estricto aun que el recogido en la actual Directiva.

Pasaremos ahora a analizar la responsabilidad aplicable a los principales agentes que pueden llegar a haber tenido algún tipo de relación con el daño causado. Quizá el sujeto que cuenta tradicionalmente con mayor relevancia es el productor o fabricante del producto. Pero una de las características que conlleva la inteligencia artificial es la aparición de una gran cantidad de sujetos, con distintas actividades y roles, que tienen relación con la creación del producto final. De este modo habrá que tener en cuenta a los desarrolladores de la inteligencia artificial, a los encargados de generar los algoritmos, a los encargados de aportar y procesar los datos, a los propiamente fabricantes de los objetos que incorporen el software de inteligencia artificial, a los propietarios de estos, y a los operadores o usuarios de los mismos, aunque algunos de ellos pudieran englobarse en una misma categoría<sup>217</sup>. Así, todos los sujetos a los que me acabo de referir podrían encajar en el concepto de productor, a excepción hecha de los propietarios del producto y los operadores del mismo, que deberán contar con sus propias normas particulares a las que ahora me referiré.

### 3.2.1. *El productor*

El artículo 3 de la Directiva 85/374 define al productor como “*la persona que fabrica un producto acabado, que produce una materia prima o que fabrica una parte integrante, y toda aquella persona que se presente como productor poniendo su nombre, marca o cualquier otro signo distintivo en el producto.*” Es evidente que este concepto, con las características que conlleva la inteligencia artificial, no engloba todos los actores que, de una forma o de otra, participan en la creación de la aplicación o del robot. Es por ello por lo que una de las principales novedades que se recoge en el informe tanto de la Comisión Europea como del Parlamento Europeo es la propuesta de modificación del concepto de productor, en el que se debería incluir a todos los agentes involucrados en la elaboración del producto. Concretamente, en su recomendación octava señala que, en el nuevo concepto de productor, deberían tener cabida “*los fabricantes, desarrolladores, programadores, proveedores de servicios y operadores finales.*”

A pesar de que la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial señale en su Considerando B que “*el concepto de productor debe incluir a fabricantes, desarrolladores, programadores, prestadores de servicios y operadores finales*”, lo cierto es que durante toda la propuesta distingue entre operadores por un lado y

---

217 GIUFFRIDA, I.: “Liability for AI decision-making: Some legal and ethical considerations.”, en *Fordham Law Review*, Vol. 88, núm. 2, pág. 443

productores por otro. Tanto es así que, en la propuesta, en su artículo 3 concretamente, define al productor de manera independiente y distinta a como lo hace con el operador. Cuestión distinta es, como señala el artículo 11 de la propuesta, ya mencionado, que el productor pudiera llegar a ser también operador, en cuyo caso le será de aplicación el Reglamento y la responsabilidad sería del tipo objetiva.

Es importante señalar a estos efectos que será considerado productor aun en el caso en el que el producto resultante de su trabajo no sea tangible, sino digital. A esta novedad me referiré al final del presente epígrafe, haciendo hincapié a la exigencia de transparencia y comprensión del software.

Respecto al sistema de responsabilidad civil que le será de aplicación al productor, como acabamos de ver, la Directiva 85/374 establece un régimen de responsabilidad cuasi objetivo o por riesgo, que hará que, con carácter general, los productores respondan por los daños producidos por los daños provocados. Ese régimen, en la propuesta elevada por la Comisión Europea, no sufre apenas modificaciones, apostando por la continuidad del sistema de responsabilidad actualmente existente, aunque diría que yendo un paso más allá en cuanto a la objetividad, como ahora explicaré, a través de la posible eliminación de exenciones hoy existentes. Incluso en el informe del Parlamento hace mención a la responsabilidad del productor a través de la establecida en la Directiva 85/374. De este modo, el informe señala que “*la responsabilidad objetiva del productor debe desempeñar un papel fundamental en la indemnización de los daños causados por productos defectuosos.*”<sup>218</sup> Como señala DÍAZ-ALABART, debido a la existencia de cierta autonomía en el ámbito de la inteligencia artificial, y a que la actividad llevada a cabo por ella conlleva un cierto grado de riesgo o peligro, lo más razonable es que la responsabilidad civil se configure como una responsabilidad objetiva<sup>219</sup>.

Actualmente la Directiva sobre las máquinas 2006/42/CE, así como la Directiva 2001/95/CE sobre la seguridad general de los productos, establecen los requisitos de seguridad que un fabricante debe respetar para la puesta en el comercio de sus productos<sup>220</sup>. Ahora, las obligaciones del productor pasarán, según se establecen en la recomendación 17 del informe de expertos, por “*diseñar, describir y comercializar los productos de forma que permitan a los operadores cumplir efectivamente con los deberes establecidos y en controlar adecuadamente el producto tras su puesta en circulación.*”<sup>221</sup> Lo mismo sucederá en el caso

218 Así se recoge en la recomendación 13 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 6

219 Vid. DÍAZ ALABART, S.: “Robots y responsabilidad civil”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018, pág. 107

220 Cfr. PALMIERI, E., “Robótica y derecho: sugerencias, confluencias, evoluciones ... Op. cit., pág. 66

221 Así se recoge en la recomendación 17 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 7

en el que los defectos del producto aparezcan con posterioridad a su puesta en circulación, siempre y cuando aquel siga siendo el responsable de las actualizaciones del producto<sup>222</sup>.

Lo que sí conlleva una novedad importante en la propuesta realizada es la exclusión, con carácter general, de la exoneración de responsabilidad del productor por los conocidos como “*riesgos del desarrollo*”, que no es otra cosa que profundizar en la objetivación del sistema de responsabilidad civil como acabo de señalar. Esta exoneración, que sí aparece en el artículo 7 de la actual Directiva 81/374<sup>223</sup> y en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios, se entiende ahora que, como señalan GÓMEZ LIGÜERRE y GARCÍA-MILCÓ, “*podría liberar de responsabilidad a buena parte de los potenciales responsables en perjuicio de las víctimas y en beneficio de productores*”<sup>224</sup>. De este modo, hay una causa de exoneración que urge eliminar. Concretamente es la establecida en el artículo 7.b que permite exonerar de responsabilidad al productor en aquellos casos en los que “*el defecto que causó el daño no existiera en el momento en que él puso el producto en circulación o que este defecto apareciera más tarde.*”

Como ya he advertido, una de las características que acompaña a la inteligencia artificial es precisamente la de ser capaz de ir aprendiendo con el tiempo o, lo que es lo mismo, de ir cambiando a través de distintos procesos. Igual sucedería con las actualizaciones que se le pudiesen ir haciendo, algo que es muy habitual en cualquier software. Si se mantiene esta causa de exoneración, el productor no sería responsable en aquellos casos en los que el daño fuese provocado por una decisión tomada en base no al software o algoritmo original, sino como consecuencia de lo aprendido por la máquina a lo largo del tiempo. Algunos autores se inclinan también por eliminar la causa de exoneración establecida en el artículo 7.e que hace referencia a que “*en el momento en que el producto fue puesto en circulación, el*

---

222 Así se recoge en la recomendación 14 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 6

223 Establece el artículo 7 de la Directiva 85/374 que “*el productor no será responsable si prueba : a) que no puso el producto en circulación*

*b) o que, teniendo en cuenta las circunstancias, sea probable que el defecto que causó el daño no existiera en el momento en que él puso el producto en circulación o que este defecto apareciera más tarde*

*c) o que él no fabricó el producto para venderlo o distribuirlo de alguna forma con fines económicos, y que no lo fabricó ni distribuyó en el ámbito de su actividad profesional*

*d) o que el defecto se debe a que el producto se ajusta a normas imperativas dictadas por los poderes públicos*

*e) o que, en el momento en que el producto fue puesto en circulación, el estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto*

*f) o que, en el caso del fabricante de una parte integrante, el defecto sea imputable al diseño del producto a que se ha incorporado o a las instrucciones dadas por el fabricante del producto”*

224 Vid. GÓMEZ LIGÜERRE, C., y GARCÍA-MILCÓ, G.: “Liability for Artificial ... Op. cit., pág. 509

*estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto*<sup>225</sup>.

Pero este sistema de responsabilidad objetiva, en el caso concreto del productor, debe contar con ciertos límites, algo que no sucederá en muchas ocasiones, como ahora explicaré, en el caso del operador. Me refiero a la necesidad de tener en cuenta que, en cualquier caso, el productor tenga la oportunidad de probar que el daño no ha sido producido por defecto de su producto, sino por otra causa. Sin duda, la causalidad deberá seguir jugando un papel fundamental a la hora de determinar la responsabilidad del productor.

Imaginemos un producto, en este caso una alarma antirrobo, dotada de un sistema de inteligencia artificial. Supongamos también que esa alarma se conecta a la red wifi del domicilio y avisa al móvil del propietario, en función de unos datos determinados, cada vez que se produce una amenaza. Pensemos que alguien hackee la red particular de ese propietario, y provoque que salte la alarma, con el consiguiente coste de tener que desplazar a un equipo para comprobar la situación de la vivienda. Si el productor puede probar que la alarma funcionaba correctamente, y que ha sido a través del wifi el medio por el que se ha provocado el daño, nada debería impedir que el productor de la alarma pudiera ser exonerado de reparar el daño causado. Posteriormente me detendré con mayor atención en la causalidad como un elemento fundamental a la hora de establecer la responsabilidad civil del productor.

### 3.2.2. *La responsabilidad civil del desarrollador del software*

Si bien es cierto que el concepto tradicional de productor se limitaba a incluir los sujetos de los que hemos hablado en el apartado anterior, la propuesta realizada por la Unión Europea ha ido un paso más allá. Me refiero al hecho de pedir que se incluya expresamente entre estos a los proveedores que, en este caso, hace también referencia a los programadores del software y a los desarrolladores de las aplicaciones con inteligencia artificial. Así pues, en lo que respecta a la inteligencia artificial, la figura del desarrollador de software cobrará una especial relevancia como se pone de manifiesto tanto en el Informe del Parlamento Europeo como de la Comisión Europea. De este modo, el Parlamento Europeo ha recomendado recientemente que “*tras la revisión de la Directiva, el concepto de «productor» debe incluir a fabricantes, desarrolladores, programadores...*”<sup>226</sup>

<sup>225</sup> Como señala CASADESUS RIPOLL, “*el principal problema en relación con esta causa de exoneración tiene que ver con la dificultad de probar, antes de su comercialización, el producto robótico en cuestión en todas las situaciones diferentes en las que se puede encontrar.*” Cfr. Vid. CASADESUS RIPOLL, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, en *Revista de la Facultad de Derecho de México*, núm. 278, 2020, pág. 367

<sup>226</sup> Vid. 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

El software se trata de un producto, bien independiente, bien unido a otro más complejo, que es el que permite realizar distintas tareas. Pensemos, por ejemplo, en un robot. Este contará con un software, que realmente será el que lo dote de inteligencia artificial, y un hardware, que sería el armazón físico. Si alguien o algo resultase dañado por el robot, podría dirigirse frente a cualquiera de ellos, por ser ambos productores. Otra cosa es que luego el creador del software pudiese repetir contra el del hardware, o viceversa, acreditando que el daño trae causa única y exclusivamente de uno de los componentes del robot.

Hay autores que sostienen que los programadores del software tan solo “*responderán de los daños provocados por los defectos del programa.*” Pero habría que matizar esta afirmación tan rotunda. Es muy posible que en muchas ocasiones coincidan las figuras del operador con las del programador del software o con el productor. En estos casos, la propuesta de Reglamento establece, como ya he mencionado anteriormente, que este “*debe prevalecer sobre la Directiva sobre responsabilidad por los daños causados por productos defectuosos.*” Esto significa que la responsabilidad sería objetiva también para el programador, siempre que nos encontremos ante una actividad peligrosa o de alto riesgo.

De otra parte, un elemento que no podemos obviar, y que dotará de mayor complejidad la determinación del responsable de los daños que pudiesen producirse por la actividad de la inteligencia artificial, es el hecho de que, a no tardar mucho, los robots podrán ir adquiriendo una complejidad tal, que serán capaces incluso de llegar a independizarse de su propio diseño original<sup>227</sup>. De ahí que los desarrolladores de software tengan un importante papel en este aspecto y deban de contribuir al fácil acceso a su trabajo. Así, en materia de inteligencia artificial se habrá de garantizar los principios de “*transparencia, auditabilidad, explicabilidad y trazabilidad*”. Se trata de otra de las novedades más relevantes de la propuesta actual y sobre la que menos se ha trabajado hasta el momento.

Así, estos elementos se convierten también en novedades muy destacadas para tener en cuenta y serán determinantes a la hora de poder establecer la correspondiente asignación de la responsabilidad civil. El segundo de los principios a los que anteriormente hacía referencia es la explicabilidad, consistente en hacer posible que el contenido de la aplicación o del software pueda ser entendido por el receptor. La transparencia, al menos así lo entiendo la Comisión Europea, hace referencia a un sistema que, de por sí, sea sencillo y entendible.

Me detendré en los principios de trazabilidad y auditabilidad, por ser esenciales en el proceso de asignación de la responsabilidad civil. El prime-

---

<sup>227</sup> Vid. GARCÍA-PRIETO CUESTA, J.: “¿Qué es un robot?”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluwer, pág. 59

ro de ellos es el referente a la trazabilidad de los algoritmos o del software. Cuando un algoritmo sea el causante del daño es necesario saber quién ha sido el que lo ha diseñado, para poder así determinar el grado de responsabilidad del programador. Como ya he afirmado, a la hora de determinar el responsable de un daño, siempre habrá, antes o después, un comportamiento humano que está detrás del mismo.

Tanto es así que en la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo denominada Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial, en el Anexo IV.2.c., se exige que se incluya información sobre “*la descripción de la arquitectura del sistema, explicando cómo los componentes de software se basan o se alimentan entre sí y se integran en el procesamiento global; los recursos informáticos utilizados para desarrollar, entrenar, probar y validar el sistema de IA*”.

Ya comenté el hecho de que en distintos países se ha impuesto la necesidad de contar en estos casos con una “*puerta trasera*” y en España, en la consulta pública de la Carta de Derechos Digitales, se hace mención expresa a esta trazabilidad. Es muy importante que la legislación establezca unas obligaciones estrictas a los fabricantes a la hora de, en caso de investigación judicial, poder tener acceso al desarrollo del software del dispositivo con inteligencia artificial, eliminando cualquier encriptación que pudiese obstaculizar la misma. Es evidente que en caso de que haya que establecer la responsabilidad civil por el daño causado, el acceso a esta prueba por parte del perjudicado es un elemento esencial a la hora de establecer el nexo causal. Señalan, con razón, SAIF y AMMANATH que para que se pueda confiar en la inteligencia artificial, “*todos los participantes tienen derecho a entender cómo se están usando sus datos y cómo la IA está tomando decisiones. Los algoritmos, atributos y correlaciones de la IA deben estar abiertos a la inspección, y sus decisiones deben ser totalmente explicables*”<sup>228</sup>.

No es un tema menor este que señalamos, pues ya se han dado bastantes casos en los que, si bien en otro orden de cosas, las autoridades judiciales no han podido acceder al contenido de un dispositivo móvil de un terrorista, por no tener la capacidad técnica para ello y al haberse negado la empresa responsable del desarrollo del dispositivo<sup>229</sup>.

Es cierto que se trata de una cuestión compleja porque, como es normal, a la empresa creadora del dispositivo le puede preocupar que se filtren las

---

228 “*A medida que las decisiones y los procesos que dependen de la IA aumentan tanto en número como en importancia, la IA ya no puede tratarse como una “caja negra” que recibe entradas y genera salidas sin una clara comprensión de lo que ocurre en su interior.*” Cfr. SAIF, I. y AMMANATH, B.: “Trustworthy AI is a framework to help manage... Op. cit.

229 Recientemente Apple se negó a desbloquear el iPhone del autor del tiroteo de Pensacola en el que hubo decenas de fallecidos. Vid. Apple no ayudará al FBI a desbloquear el iPhone del tiroteo de Pensacola. (2020). *El Español*. Accesible en [https://www.elespanol.com/omicro/20200114/apple-no-ayudara-fbi-desbloquear-tiroteo-pensacola/459704553\\_0.html](https://www.elespanol.com/omicro/20200114/apple-no-ayudara-fbi-desbloquear-tiroteo-pensacola/459704553_0.html)

características del sistema operativo o software de este cuyas consecuencias empresariales pueden ser de un coste muy elevado. Hablamos de miles de millones de euros en juego, por lo que la legislación debería establecer también algunas medidas para asegurar por un lado el acceso al contenido a las autoridades judiciales y, por otro, la protección de la propiedad intelectual del mismo. En este sentido, varios países de la Unión Europea ya han reclamado la necesidad de establecer por ley estas *puertas traseras* en una futura regulación europea<sup>230</sup>.

Como señala la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, ninguna de las definiciones ha sido aun aceptada de manera universal, el gran problema en este sentido será de índole probatoria, ya que los afectados podrían verse en la situación de no ser capaces de determinar la responsabilidad al carecer de disposiciones específicas<sup>231</sup>.

En definitiva, y a modo de resumen, los creadores de un software, o los desarrolladores del producto, pasarán en la futura legislación a ser incluidos en el concepto de productor, asumiendo así la misma responsabilidad que a este se le asigna en la actual Directiva. Así pues, el que dota de un software tal que permita que las aplicaciones o los robots se independicen del diseño original del fabricante deberá también asumir los riesgos que esta autonomía o independencia pueda conllevar por lo que, aunque no sería responsable por vía directa de esos hechos, sí que lo sería por vía indirecta a través de la responsabilidad civil por riesgo. Así lo recomienda el Parlamento Europeo en su informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial apuesta por “*aplicar un régimen de responsabilidad justa a los fallos de los programas operativos, los fallos de red y los riesgos relacionados con las opciones de programación que actualmente no están adecuadamente cubiertas.*” A ello hay que añadirle el hecho de que los desarrolladores de software podrán actuar también en ocasiones como operadores, por lo que su responsabilidad, en dichas circunstancias, para los casos en los que sean de alto riesgo o peligrosos, sería plenamente objetiva.

Hay autores que defienden que es necesario que cualquier producto dotado con inteligencia artificial señale de forma clara quién es el responsable en caso de que éste provoque un daño a terceros. Ponen el ejemplo de un ciudadano que utilice los servicios de una empresa cuyos productos van destinados a la realización de inversiones a través de una aplicación con inteligencia artificial, y que, debido a los malos algoritmos utilizados en ella, pierde sus ahorros. Sostienen que “*debería haber un mecanismo para identificar*

---

230 Alemania prepara una ley para que existan “puertas traseras” en cualquier dispositivo moderno. (2017). *Derecho De La Red*. Accesible en <https://derechodelared.com/alemania-ley-puertas-traseras/>

231 Cfr. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (2018), *Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial*, pág. 3

*quién es responsable del daño*”<sup>232</sup>. No comparto esa necesidad de que los creadores del algoritmo, los programadores, tengan que ser señalados a priori, pero sí que puedan llegar a serlo en el caso en el que se provoque un daño.

Y ello porque no debe hacerseles automáticamente responsables de los daños, a excepción del caso señalado en el que sean también los operadores del sistema de alto riesgo. Por dos motivos: En primer lugar, porque nos encontraríamos, no ya la inversión de la carga de la prueba que es admitida ampliamente por la doctrina en los casos de responsabilidad por riesgo, sino ante una *probatio diabólica*. Por el mero hecho de ser el autor del software, eres el responsable del daño causado. Lo que nos lleva también a que chocaría con otro de los principales problemas que nos encontraremos en el ámbito de la responsabilidad civil en la inteligencia artificial, que no es otro que el de la relación de causalidad. Antes de determinar el responsable del daño será necesario establecer que la causa del daño fue, al menos en parte, por el algoritmo que determina las acciones de la aplicación. Pensemos, por ejemplo, que la aplicación hubiese sido pirateada por un tercero, y esa acción fuese la que hubiese generado la pérdida patrimonial y no el algoritmo. Otra cosa sería determinar si el hecho de que la aplicación pudiese ser pirateada podría también ser un motivo, debido a una posible falta de diligencia, por el que culpabilizar al autor de la misma.

Otro problema que se plantea es el de determinar quién es, en caso de que el daño sea provocado por el software, el que debe de responder por el mismo. Así, surge el interrogante de si deberá ser responsable el autor del software, o el titular de los derechos del mismo. KINGSTON plantea esta cuestión en un sentido amplio, al afirmar que, si el software es el responsable del daño, no solo podría ser culpa del programador, sino que incluye también “*el diseñador del programa; el experto que proporcionó los conocimientos; o el gestor que designó al experto, al diseñador del programa o al programador inadecuados*”<sup>233</sup>. En mi opinión tiene que ser el titular del mismo, siempre que obtenga un beneficio por la cesión o venta del mismo, pues ha de asumir el riesgo que le aportan tales beneficios. Otra cosa es que se trate de una responsabilidad solidaria y pueda repetir contra el programador en el caso en el que pueda determinarse la relación de causalidad.

### 3.2.3. Responsabilidad civil del operador

A los sujetos ya mencionados a los que se les podrá atribuir responsabilidad civil, habría que sumar uno determinante, que aparece como novedad en la propuesta de Reglamento realizada por los expertos a la Comisión y

<sup>232</sup> Cfr. Cfr. SAIF, I. y AMMANATH, B.: “Trustworthy AI is a framework to help manage... Op. cit.

<sup>233</sup> KINGSTON, J.: Artificial Intelligence and Legal Liability, *International Conference on Innovative Techniques and Applications of Artificial Intelligence*, 2016, pág. 13

recogida también en la recomendación del Parlamento Europeo. Hablamos del operador, que será aquel que controle el riesgo que produzca la inteligencia artificial y que a su vez obtenga algún tipo de beneficio por su uso. La propuesta de Reglamento aprobada por el Consejo Europeo y el Parlamento Europeo en materia de responsabilidad civil incluye dentro de la figura del operador al proveedor, al usuario, al representante autorizado, al importador y al distribuidor

Esta propuesta distingue entre operador inicial, que será cualquier persona, ya sea física o jurídica, que ejerza algún tipo de control “sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento” y operador final que será aquel que “defina las características de la tecnología y proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA”<sup>234</sup>.

Tanto la Comisión Europea como el Parlamento Europeo han justificado la inclusión de este nuevo sujeto en la futura legislación sobre responsabilidad civil causada por la inteligencia artificial. Concretamente, el Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial del Parlamento Europeo, sostiene que “la responsabilidad civil del operador se justifica por el hecho de que controla un riesgo asociado al sistema de IA, comparable al del propietario de un automóvil”<sup>235</sup>. Este sujeto, actualmente se rige por las reglas generales de la responsabilidad civil, bien sea la referida a la responsabilidad civil extracontractual o la responsabilidad civil contractual.

En este sentido, como ya he señalado, recientemente se ha presentado la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo denominada Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial, que fue publicada el 21 de abril de 2021. La principal novedad en este aspecto se refiere al establecimiento de una triple división entre los distintos sistemas de inteligencia artificial: prohibidos, de alto riesgo y aquellos que no son ni prohibidos ni de alto riesgo. Dependiendo de ante cuál de ellos nos encontremos, el sistema de responsabilidad civil será objetivo o subjetivo.

El primer bloque se refiere a los sistemas de inteligencia artificial prohibidos, detallados ampliamente en el artículo 5.1, que, a grandes rasgos, serán aquellos que tengan como objetivo manipular o explotar las debilidades o circunstancias especiales de las personas<sup>236</sup>. También se prohíbe el uso

---

<sup>234</sup> Arts. 3 e) y f) de la propuesta de Reglamento recogido en el *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*

<sup>235</sup> Vid. Parlamento Europeo (2020), *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*, pág. 9

<sup>236</sup> Artículo 5

1. Quedan prohibidas las siguientes prácticas de inteligencia artificial:

de esta técnica para llevar a cabo una “*vigilancia indiscriminada de las personas físicas*” y como elemento clave para la toma de decisiones que restrinjan los derechos y libertades fundamentales. Esta prohibición general tendrá la única excepción de aquellos casos en los que las autoridades públicas, con el fin de salvaguardar la seguridad, lleven a cabo su uso siempre y cuando se garanticen los derechos y libertades.

El segundo bloque al que hacía ahora referencia es el relativo a los sistemas de inteligencia artificial de alto riesgo. Para la clasificación de este tipo de sistemas, que son clave en lo que a responsabilidad civil se refiere, la propuesta de Reglamento incluye el Anexo III, en el que se detallan las prácticas de inteligencia artificial clasificadas como tales, así como la posibilidad de que, a través de la creación de un Comité Europeo de Inteligencia Artificial, determine nuevas prácticas que pasarían a formar parte del

---

(a) la comercialización, puesta en servicio o uso de un sistema de IA que despliegue técnicas subliminales más allá de la conciencia de una persona con el fin de distorsionar materialmente el comportamiento de una persona de manera que cause o pueda causar a esa persona o a otra un daño físico o psicológico;

(b) la comercialización, puesta en servicio o utilización de un sistema de IA que explote cualquiera de las vulnerabilidades de un grupo específico de personas debido a su edad, discapacidad física o mental, con el fin de distorsionar materialmente el comportamiento de una persona perteneciente a ese grupo de manera que cause o pueda causar un daño físico o psicológico a esa persona o a otra;

(c) la comercialización, puesta en servicio o utilización de sistemas de IA por parte de las autoridades públicas o en su nombre para la evaluación o clasificación de la fiabilidad de las personas físicas durante un determinado período de tiempo, sobre la base de su comportamiento social o de sus características personales o de personalidad conocidas o previstas, con la puntuación social que conduce a una de las siguientes situaciones o a ambas:

(i) tratamiento perjudicial o desfavorable de determinadas personas físicas o grupos enteros de las mismas en contextos sociales que no guardan relación con los contextos en los que se generaron o recogieron originalmente los datos;

(ii) el tratamiento perjudicial o desfavorable de determinadas personas físicas o grupos enteros de ellas que no esté justificado o sea desproporcionado con respecto a su comportamiento social o a su gravedad;

(d) el uso de sistemas de identificación biométrica a distancia “en tiempo real” en espacios de acceso público con fines policiales, a menos y en la medida en que dicho uso sea estrictamente necesario para uno de los siguientes objetivos;

(i) la búsqueda selectiva de posibles víctimas específicas de delitos, incluidos los niños desaparecidos;

(ii) la prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de personas físicas o de un ataque terrorista;

(iii) la detección, localización, identificación o enjuiciamiento de un autor o sospechoso de un delito contemplado en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI 62 del Consejo y sancionado en el Estado miembro de que se trate con una pena o una medida de seguridad privativa de libertad de un máximo de al menos tres años, según determine la legislación de dicho Estado miembro.

citado Anexo III<sup>237</sup>. La propuesta de Reglamento se ha basado en tres criterios fundamentales para determinar este tipo de actividades: Por un lado, en la finalidad del sistema en sí misma y, por otro, en los posibles daños que pueda llegar a causar, así como en la gravedad y probabilidad de estos<sup>238</sup>.

El último de la clasificación serán aquellos sistemas de inteligencia artificial que no se encuadren en los prohibidos ni en los peligrosos cuyo margen, después de la amplia clasificación a la que haré mención ahora, es muy estrecho y se reservará para actividades menores y que no sean susceptibles de generar controversia.

Por lo que respecta a la responsabilidad civil en este ámbito, coexistirán dos sistemas de responsabilidad civil distintos. Por un lado, aquellos casos en los que nos encontremos ante un sistema de inteligencia artificial prohibido o peligroso, de riesgo elevado como lo denomina el Libro Blanco sobre inteligencia artificial de la Comisión Europea, y, por otro, para aquellos que no los sean. Para los dos primeros casos, como ahora pasará a explicar, se ha diseñado un sistema objetivo de responsabilidad civil, mientras que para el segundo será subjetivo.

Me centraré ahora en el estudio de los sistemas de inteligencia artificial peligrosos o de alto riesgo, con el objeto de precisar con mayor detalle las características y consecuencias en lo que a responsabilidad civil se refiere. La primera de ellas es que la inteligencia artificial sea empleada en un ámbito en el que sea previsible concurren riesgos significativos. En el ya mencionado Libro Blanco sobre inteligencia artificial establecen sectores como la sanidad, el transporte, la energía y el sector público que pueden tener especial incidencia<sup>239</sup>. La segunda de estas es la que se refiere a que esa inteligencia artificial se use de tal forma que puedan aparecer riesgos significativos. Es decir, que, si bien algunos ámbitos como los ahora mencionados pueden ser considerados como de riesgo, puede que la inteligencia artificial sea usada para un tema que no implique riesgo. El propio Libro Blanco señala un ejemplo clarificador en el ámbito del sector sanitario que, si bien es un sector complejo, un error del sistema de inteligencia artificial por el que se asignan las citas de un centro de salud no implicaría riesgo alguno<sup>240</sup>.

---

237 El artículo 7.1 de la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo por el que se establecen normas armonizadas sobre la inteligencia artificial señala que “*La Comisión está facultada para ... actualizar la lista del anexo III añadiendo sistemas de IA de alto riesgo cuando se cumplan las dos condiciones siguientes...*”

238 El Art. 6 de la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo por el que se establecen normas armonizadas sobre la inteligencia artificial establece que “*las reglas de clasificación para los sistemas de IA de alto riesgo*”

239 Vid. Comisión Europea, *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, 2020, pág. 21

240 Vid. Comisión Europea, *Libro Blanco sobre la inteligencia artificial...*, op. cit., pág. 21

A pesar de que el informe del Parlamento y de la Comisión señalen que el Reglamento sobre responsabilidad civil detallaría los sistemas artificiales de alto riesgo, estos se han incluido ya en el Anexo III de la propuesta de Reglamento sobre Inteligencia Artificial del Consejo Europeo y el Parlamento Europeo denominada Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial. Básicamente hace referencia a la identificación y categorización biométrica de personas físicas, la gestión y explotación de infraestructuras críticas, la educación y formación profesional, el empleo, la gestión de trabajadores y acceso al autoempleo, el acceso y disfrute de servicios privados esenciales y de servicios y prestaciones públicas, la aplicación de la ley, la gestión de la migración, el asilo y el control de fronteras y la administración de justicia y procesos democráticos. En definitiva, un amplio y detallado catálogo de actividades que serán consideradas de alto riesgo, además de las que puedan ser añadidas en el futuro a través del grupo de expertos al que antes hacía mención<sup>241</sup>.

---

241 Los sistemas de inteligencia artificial de alto riesgo recogidos en el Anexo III son:

1. Identificación y categorización biométrica de personas físicas:

a) Sistemas de IA destinados a ser utilizados para la identificación biométrica a distancia “en tiempo real” y “a posteriori” de personas físicas;

2. Gestión y explotación de infraestructuras críticas:

a) Sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y explotación del tráfico rodado y el suministro de agua, gas, calefacción y electricidad.

3. Educación y formación profesional:

(a) Sistemas de IA destinados a ser utilizados para determinar el acceso o la asignación de personas físicas a centros educativos y de formación profesional;

b) los sistemas de IA destinados a ser utilizados para evaluar a los estudiantes en los centros de enseñanza y de formación profesional y para evaluar a los participantes en las pruebas exigidas habitualmente para la admisión en los centros de enseñanza.

4. Empleo, gestión de trabajadores y acceso al autoempleo:

(a) Sistemas de IA destinados a ser utilizados para la contratación o selección de personas físicas, especialmente para la publicación de vacantes, el cribado o filtrado de solicitudes, la evaluación de candidatos en el curso de entrevistas o pruebas;

(b) la IA destinada a la toma de decisiones sobre la promoción y la finalización de las relaciones contractuales relacionadas con el trabajo, para la asignación de tareas y para el seguimiento y la evaluación del rendimiento y el comportamiento de las personas en dichas relaciones.

5. Acceso y disfrute de servicios privados esenciales y de servicios y prestaciones públicas:

(a) Los sistemas de IA destinados a ser utilizados por las autoridades públicas o en nombre de ellas para evaluar el derecho de las personas físicas a las prestaciones y servicios de asistencia pública, así como para conceder, reducir, revocar o reclamar dichas prestaciones y servicios;

(b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de las personas físicas o establecer su puntuación de crédito, con la excepción de los sistemas de IA puestos en servicio por proveedores a pequeña escala para su propio uso;

(c) Sistemas de IA destinados a ser utilizados para despachar, o para establecer la prioridad en el despacho de servicios de primera respuesta de emergencia, incluidos los bomberos y la ayuda médica.

En la propuesta de Reglamento sobre Inteligencia Artificial se detallan los daños que puede causar la inteligencia artificial, que incluyen los siguientes: Las lesiones o muerte; Los daños provocados en la propiedad privada; Los impactos adversos sistémicos para la sociedad en general; Las interrupciones significativas en la prestación de servicios esenciales; El impacto en las oportunidades financieras, educativas o profesionales; El impacto en el

---

6. Aplicación de la ley:

a) Los sistemas de IA destinados a ser utilizados por las autoridades policiales para realizar evaluaciones individuales del riesgo de las personas físicas con el fin de evaluar el riesgo de que una persona física delinca o reincida o el riesgo para las posibles víctimas de delitos;

b) Sistemas de IA destinados a ser utilizados por las autoridades policiales como polígrafos y herramientas similares o para detectar el estado emocional de una persona física;

c) los sistemas de IA destinados a ser utilizados por las autoridades policiales para detectar falsificaciones profundas, tal como se menciona en el artículo 52, apartado 3;

d) sistemas de IA destinados a ser utilizados por las autoridades policiales para evaluar la fiabilidad de las pruebas en el curso de la investigación o el enjuiciamiento de delitos;

e) Sistemas de IA destinados a ser utilizados por las autoridades policiales para predecir la ocurrencia o reincidencia de una infracción penal real o potencial basada en la elaboración de perfiles de personas físicas, tal como se contempla en el artículo 3, apartado 4, de la Directiva (UE) 2016/680, o para evaluar los rasgos y características de la personalidad o el comportamiento delictivo anterior de personas físicas o grupos;

f) Los sistemas de IA destinados a ser utilizados por las autoridades policiales para la elaboración de perfiles de personas físicas según lo dispuesto en el artículo 3, apartado 4, de la Directiva (UE) 2016/680 en el curso de la detección, investigación o enjuiciamiento de delitos;

g) sistemas de IA destinados a ser utilizados para el análisis de la delincuencia en relación con las personas físicas, que permitan a las autoridades policiales buscar grandes conjuntos de datos complejos, relacionados y no relacionados, disponibles en diferentes fuentes de datos o en diferentes formatos de datos, con el fin de identificar patrones desconocidos o descubrir relaciones ocultas en los datos.

7. Gestión de la migración, el asilo y el control de fronteras:

(a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes como polígrafos y herramientas similares o para detectar el estado emocional de una persona física;

b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes para evaluar un riesgo, incluido un riesgo para la seguridad, un riesgo de inmigración irregular o un riesgo para la salud, planteado por una persona física que pretende entrar o ha entrado en el territorio de un Estado miembro;

(c) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes para la verificación de la autenticidad de los documentos de viaje y de la documentación justificativa de las personas físicas y detectar los documentos no auténticos mediante la comprobación de sus características de seguridad;

(d) Sistemas de IA destinados a asistir a las autoridades públicas competentes en el examen de las solicitudes de asilo, visado y permisos de residencia, así como de las reclamaciones asociadas en relación con la elegibilidad de las personas físicas que solicitan un estatuto.

8. Administración de justicia y procesos democráticos:

(a) Sistemas de IA destinados a asistir a una autoridad judicial en la investigación e interpretación de los hechos y la ley y en la aplicación de la ley a un conjunto concreto de hechos.

acceso a los servicios públicos y a cualquier forma de asistencia pública y el impacto adverso en los derechos fundamentales.

Pasando ahora al aspecto concreto relacionado con la responsabilidad civil para estos sistemas peligrosos, la doctrina coincide con la necesidad de determinar el tipo de sistema de responsabilidad civil en base a la clase de inteligencia artificial ante el que nos encontremos. Así, GIUFFRIDA mantiene que no podrá tratarse igual a aquellos casos en los que el sistema se limite a proporcionar datos, informaciones o predicciones en los que una persona física se base para tomar una decisión, que en los que la decisión sea absolutamente autónoma<sup>242</sup>. Como ya he señalado, se ha incluido en el Anexo III de la Propuesta de Reglamento, de manera exhaustiva, todos esos sistemas complejos de inteligencia artificial que darían lugar a la aplicación del sistema de responsabilidad objetiva de manera directa para los operadores. El informe del Parlamento Europeo define estos sistemas complejos como aquellos que cuentan con un *“potencial significativo en un sistema de IA que funciona de forma autónoma para causar daños o perjuicios a una o más personas de manera aleatoria y que excede lo que cabe esperar razonablemente; la magnitud del potencial depende de la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía de la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y el contexto en que se utiliza el sistema de IA”*.

Como decía antes, para este nuevo sujeto, el operador, se propone en el Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, en este caso sí, un sistema de responsabilidad civil absolutamente objetivo, siempre y cuando nos encontremos ante el uso de un sistema de inteligencia artificial *complejo* o de alto riesgo. Refiere el informe que *“la responsabilidad objetiva debe recaer en la persona que controla el riesgo relacionado con el funcionamiento de las tecnologías digitales emergentes y que se beneficia de su funcionamiento (operador)”*<sup>243</sup>. Así, será su obligación la de seleccionar cuidadosamente el sistema que usarán, y por el que obtendrán beneficios, deberá contar con la capacidad de controlarlo -lo que incluye en su caso tener las competencias o habilidad para su uso- y realizar un correcto mantenimiento<sup>244</sup>.

Hasta tal punto será objetiva que se prevé que los operadores no puedan eximirse de la responsabilidad de los daños causados en ningún caso, excepción hecha de los daños producidos por fuerza mayor. Es decir, ni si quiera se podrían eximir de la responsabilidad acreditando su actuación con la diligencia debida. Así se plasma en el artículo 4.3. de la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destina-

---

242 GIUFFRIDA, I.: “Liability for AI decisión-making... Op. cit., pág. 444

243 Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 39

244 Vid. Vid. GÓMEZ LIGÜERRE, C., y GARCÍA-MILCÓ, G.: “Liability for Artificial ... Op. cit., pág. 508

das a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial: “*Los operadores de un sistema de IA de alto riesgo no podrán eludir su responsabilidad civil alegando que actuaron con la diligencia debida o que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA. Los operadores no serán responsables si el daño o perjuicio ha sido provocado por un caso de fuerza mayor.*” Se trata pues, de un cambio determinante en el sistema de responsabilidad civil tradicional, que garantizará la protección de los usuarios a costa de privar a los operadores de la posibilidad de demostrar su falta de responsabilidad. Como posteriormente expondré, ello vendrá acompañado de una exigencia para los operadores de contratación de un seguro de responsabilidad civil obligatorio.

En cambio, si el sistema de inteligencia artificial que causa el daño no se trata de un sistema de alto riesgo, nos encontraremos ante una responsabilidad civil subjetiva. Para poder llegar a esquivar la responsabilidad civil deberá acreditar que no tuvo la culpa del daño en base a dos motivos. El primero si el sistema de inteligencia artificial se activó sin su conocimiento y consentimiento, habiendo, eso sí, establecido las medidas razonables para evitar esa activación inintencionada. El segundo de los motivos será aquel por el cual se pueda acreditar que “*observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA apropiado para las tareas y las capacidades adecuadas, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles*”<sup>245</sup>.

Como ya he comentado, la legislación europea y española va en la línea de la necesaria participación del ser humano en la toma de decisiones, o en el control de estas, por lo que estos sujetos, los operadores, son tenidos en cuenta como responsables de los daños producidos. De este modo, si llega a materializarse lo propuesto en la Carta de Derechos digitales, esa participación tendrá carácter imperativo. En este sentido, el documento otorga el derecho a cualquier persona de que las decisiones tomadas de manera automática por la inteligencia artificial puedan ser supervisadas y contar con la intervención de las mismas por parte del ser humano. Ello podría atenuar la responsabilidad civil del fabricante, puesto que permite trasladar parte de esa responsabilidad al supervisor u operador humano. Si aquel que ha recibido el daño renuncia al derecho de exigir que la decisión sea revisada por un ser humano, que forme parte de la entidad que haya tomado la decisión, no podrá responsabilizar a esa entidad, puesto que ha renunciado al ejercicio de un derecho.

Otra de las circunstancias que debemos plantearnos es la posibilidad de que el encargado de revisar esas decisiones propuestas por la inteligencia artificial no llegue a hacerlo. Si se estuviese a tiempo de reparar el daño, el

---

<sup>245</sup> Art. 8.2 de la propuesta de Reglamento recogido en el *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*

afectado podría reclamar la revisión de la decisión. Pero si el daño ya se hubiese producido, la responsabilidad directa de aquel que incumplió el deber de controlar o supervisar la decisión sería incuestionable.

Por otro lado es necesario, en mi opinión, que la responsabilidad del operador esté ligada a la del productor a través del establecimiento de una obligación solidaria entre ambos, en la que el afectado pueda reclamar a cualquiera de ellos, con lo que se satisfaría el principal objetivo que no es otro que la reparación del daño, y que, a posteriori, el operador pueda repercutir frente al productor, o viceversa, determinándose también la posible cuota de responsabilidad que habría que asumir definitivamente cada uno de ellos. Así se prevé en la propuesta de Reglamento del Parlamento Europeo, cuyo artículo 11 establece que “*en caso de que haya más de un operador de un sistema de IA, estos serán responsables conjuntos y solidarios.*”

### **3.3. La necesaria actualización de conceptos recogidos en la Directiva 85/374**

Ya he señalado que la futura legislación europea relativa a productos defectuosos ha de modificar el contenido relativo a los sujetos que deberán ser incluidos entre los productores. Pero no será lo único que deba de ser actualizado. Así, los actuales conceptos de producto, daño o defecto deben de ser revisados para poder actualizarlos a las circunstancias actuales que distan mucho de las existentes anteriormente.

Una de las circunstancias que según la Comisión Europea urge afrontar es la relativa a la definición de producto que realiza la actual Directiva sobre responsabilidad por los daños causados por productos defectuosos puesto que, en su opinión, es demasiado amplia y genérica y ello podría implicar dejar fuera de su aplicación a las empresas responsables de llevar a cabo los programas informáticos<sup>246</sup>. El artículo 2 de la mencionada Directiva define al producto como “*cualquier bien mueble, excepto las materias primas agrícolas y los productos de la caza, aun cuando está incorporado a otro bien mueble o a uno inmueble.*” Pero, en lo que respecta al presente estudio, ¿podría incluirse la inteligencia artificial en la definición de producto recogida en la actual legislación? A este respecto ha existido un amplio debate doctrinal y ha generado ciertas vacilaciones en las propias instituciones europeas. De este modo, en la Evaluación de la Directiva 85/374 se llega a afirmar que “*existen algunas dudas sobre la posibilidad de considerar un software de código abierto como un producto de conformidad con el artículo 2 de la Directiva*”<sup>247</sup>.

---

<sup>246</sup> Comisión Europea: *Informe de la Comisión Europea al Parlamento Europeo sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*, 2020

<sup>247</sup> Vid. *Evaluación de la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de la responsabilidad por productos defectuosos*, 2018, pág. 37

En mi opinión, no se trata tanto, como sostiene una parte de la doctrina, de que el software no se pueda incluir en el concepto de producto recogido en la Directiva por ser un bien inmaterial, puesto que tanto los robots como el software serían considerados como bienes muebles, los primeros materiales y los últimos inmateriales. Como señala ARIAS DE RINCÓN, “*el programa como un bien inmaterial, regulado por el Derecho de autor y sobre el cual se transmiten derechos de propiedad intelectual, por el otro, los datos electrónicos que contienen el programa, datos electrónicos susceptibles de ser considerados cosas bienes muebles incorpóras*”<sup>248</sup>. Tanto es así que algunos países, como Estonia y Francia, han reconocido que el software se trata de un producto y como tal, a los daños que puedan llegar a producir les sería de aplicación lo recogido en la Directiva 85/374<sup>249</sup>. Es más, el software es reconocido como producto en Reglamento 2017/745 sobre los productos sanitarios y en el Reglamento 2017/746 sobre los productos sanitarios para diagnóstico in vitro<sup>250</sup>.

En cambio, sí que plantea más dudas su inclusión en el concepto actual el hecho de que los productos basados en el uso de la inteligencia artificial sean altamente complejos. Sobre este particular, ya en la evaluación que realizó el Consejo Europeo de la aplicación de la Directiva 85/374 se advertía de la práctica imposibilidad para la aplicación de la definición de producto defectuoso en estos casos<sup>251</sup>. Parece evidente que, en lo que respecta a los productos dotados con software basados en la inteligencia artificial, tendrán un carácter especialmente complejo, por lo que, aunque la Directiva haya funcionado correctamente, es conveniente que, como señala el informe ahora mencionado, se produzca una modificación de la definición de producto en la próxima legislación.

También se hace necesario llevar a cabo una actualización del concepto de daño. Actualmente, el artículo 9 de la Directiva 85/374 prevé tanto los daños físicos, ya sea el fallecimiento o las lesiones, como los patrimoniales, definidos como los daños causados a una cosa o la destrucción de esta. Pero son varios los autores que sostienen la necesidad de ampliar el actual concepto de daño para adecuarlos con claridad a los que puedan ser

---

248 Vid. ARIAS DE RINCÓN, M.I.: “La calificación jurídica de las transmisiones de software en Internet”, en *Frónesis*, vol.14, núm.1, 2007, pág. 13

249 Vid. *Evaluación de la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de la responsabilidad por productos defectuosos*, 2018, pág. 37

250 Vid. CASADESUS RIPOLL, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, en *Revista de la Facultad de Derecho de México*, núm. 278, 2020, pág. 359

251 Vid. *Evaluación de la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de la responsabilidad por productos defectuosos*, 2018, pág. 25

provocados por la inteligencia artificial<sup>252</sup>. De este modo, la propuesta de Reglamento realizada por el Parlamento Europeo prevé definir el daño o perjuicio como “*el impacto adverso que afecta a la vida, la salud, la integridad física de una persona física, los bienes de una persona física o jurídica o bien que produce daños morales significativos que resultan en una pérdida económica verificable*”<sup>253</sup>.

Es cierto que no se prevé de forma expresa la reparación de esos daños por la legislación europea actual, pero también lo es que permite que sea recogida por las legislaciones nacionales al afirmar en el artículo 9 que “*el presente artículo no obstará a las disposiciones nacionales relativas a los daños inmateriales.*” No obstante, el legislador español optó por excluir expresamente la posibilidad de reclamar por daños morales, remitiendo a las reglas generales de responsabilidad contractual y extracontractual. Así lo dispone el artículo 128 del Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios: “*Las acciones reconocidas en este libro no afectan a otros derechos que el perjudicado pueda tener a ser indemnizado por daños y perjuicios, incluidos los morales, como consecuencia de la responsabilidad contractual, fundada en la falta de conformidad de los bienes o servicios o en cualquier otra causa de incumplimiento o cumplimiento defectuoso del contrato, o de la responsabilidad extracontractual a que hubiere lugar.*” Debemos, por lo tanto, plantear esta cuestión ante la posibilidad de que la toma de decisiones basada en la inteligencia artificial produzca un aumento significativo de este tipo de daños.

Otro de los aspectos que ha de ser revisado es el relativo a lo que entiende por “*puesta en circulación*”, con el objetivo en este caso de tener en cuenta que, en las actuales circunstancias, los productos son susceptibles de cambiar y ser modificados con cierta facilidad, lo que aumenta la complejidad a la hora de la imputación del daño. El informe del Parlamento Europeo sostiene que es necesario abrir el debate sobre si el concepto de momento en que el producto se puso en circulación es el adecuado en el caso de las tecnologías digitales emergentes.

Por último, otro de los conceptos que debe de ser actualizado es el de defecto. La Directiva 85/374 no recoge expresamente una definición del mismo, algo que sería conveniente introducir aprovechando la reforma prevista.

### 3.4. La relación de causalidad

Otro punto complejo es el que afecta a la causalidad en un doble aspecto. El primero de ellos es en base a qué se puede determinar cuál de todos los

---

252 Sostiene CASADESUS RIPOLL que “*se hace necesaria una actualización de la noción de perjuicio que refleje las complejidades generadas por estas aplicaciones de software y algoritmos concebidos para la toma de decisiones en entornos digitales.*” Vid. CASADESUS RIPOLL, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, en *Revista de...* op. cit., pág. 363

253 Art. 3.i) de la propuesta de Reglamento recogido en el *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*

actores involucrados es el responsable del daño causado, puesto que, como ya hemos visto, tanto los programas dotados con inteligencia artificial pueden llegar a estar compuestos por múltiples dispositivos, como los actores implicados pueden ser varios. Todo ello podría dificultar, técnica y económicamente, la determinación del causante del daño. Por otro lado, y como se recoge en el informe de la Comisión Europea, el uso masivo de datos y la opacidad de los algoritmos en la toma de decisiones, pueden también complicar la determinación de las causas de los daños provocados.

Aunque Directiva 85/374 haya dado respuesta, y lo sigue haciendo aun hoy, a las principales problemáticas referidas al resarcimiento de los daños provocados por productos defectuosos, no podemos obviar que la propia Comisión Europea, en la evaluación que hizo de la mencionada Directiva en el año 2018, señaló que “*uno de los motivos más frecuentes para rechazar reclamaciones se refieren a la prueba del defecto y su relación con el daño, que en conjunto representan el 53% de los casos de rechazo*”<sup>254</sup>. Como ya he puesto de manifiesto, este problema no lo encontraremos en el caso de los operadores de sistemas de inteligencia artificial complejos o de alto riesgo, pues la responsabilidad será objetiva. No obstante, sí que tendrá relevancia en aquellos casos en los que no se trate de este tipo de tecnología de alto riesgo y en el caso de los productores.

Esta circunstancia a la que hago mención tiene aún más relevancia si cabe en el ámbito de la inteligencia artificial, puesto que, debido a la alta complejidad que conlleva su aplicación, será muy difícil que los afectados puedan llegar a probar la causa por la que se produjo el daño. Es por ello por lo que la propuesta llevada a cabo por el grupo de expertos seleccionado por la Comisión Europea, aunque mantenga el principio general por el que la víctima debe de probar la causa del daño, opta por establecer tres escenarios muy amplios en los que se eximirá de la necesidad de realizar esa prueba al afectado<sup>255</sup>.

El primero de los supuestos en los que se eximirá de la necesidad de aportar esa prueba será en los casos en los que no se dé a la víctima “*un acceso razonable a la información*” del producto, lo que generará una presunción *iuris tantum* de que el daño fue producido y la causa fue la del producto<sup>256</sup>. Esto entronca con lo que mencioné anteriormente de la trazabilidad y necesidad de transparencia en todo lo que se refiere a la programación de estos sistemas.

---

254 Vid. *Evaluación de la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de la responsabilidad por productos defectuosos*, 2018, pág. 25

255 Así se recoge en la recomendación 25 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 8

256 Así se recoge en la recomendación 22 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 7

Exime también de esa prueba en los casos en los que no sea posible, por cualquier circunstancia, identificar a aquellos que manipularon los dispositivos y realizaron modificaciones en su software o algoritmos, más allá de los establecidos por el fabricante o proveedor original.

La tercera hace referencia al establecimiento de una serie de circunstancias en las que se podría -se trata de una posibilidad, no de una imposición- establecer la inversión de la carga de la prueba. Dicho de otro modo, se entendería que existe relación de causalidad entre el defecto y el daño producido. Esas circunstancias son:

- “(a) la probabilidad de que la tecnología haya contribuido al menos al daño;*
- (b) la probabilidad de que el daño haya sido causado por la tecnología o por alguna otra causa dentro del mismo ámbito;*
- (c) el riesgo de un defecto conocido en la tecnología, aunque su impacto causal real no sea evidente;*
- (d) el grado de trazabilidad e inteligibilidad a posteriori de los procesos dentro de la tecnología que pueden haber contribuido a la causa (asimetría informativa);*
- (e) el grado de accesibilidad y comprensibilidad a posteriori de los datos recogidos y generados por la tecnología;*
- (f) el tipo y el grado de daño potencial y realmente causado”<sup>257</sup>.*

La última de las circunstancias por la que se podría eximir de la necesidad de probar este nexo será en aquellos casos en los que se incumplan las normas de seguridad que hubiesen permitido evitar el daño causado<sup>258</sup>.

### **3.5. Seguro, límite de la cuantía y plazo de prescripción**

Por lo que respecta a la posibilidad de establecer un seguro de responsabilidad civil obligatorio, el Parlamento Europeo ya se mostró favorable a establecer un régimen de este tipo, cuya obligación recaería sobre el productor de los robots y que, a diferencia del seguro de automóviles, *“debería tener en cuenta todas las responsabilidades potenciales en la cadena”<sup>259</sup>*. Aunque esta postura, como ahora explicaré ha sido modificada puesto que no es tanto al productor al que le corresponde contratar ese seguro de responsabilidad civil obligatoria, sino a los operadores.

Por otro lado hemos de señalar que a lo largo de estos años se han ido estableciendo unos límites a la hora de asegurar este tipo de daños. Las cuan-

<sup>257</sup> Así se recoge en la recomendación 26 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 8

<sup>258</sup> Así se recoge en la recomendación 24 del Informe de responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, pág. 7

<sup>259</sup> Cfr. Parlamento Europeo (2017), *Informe con recomendaciones...*, Op. cit. pág. 22

tías indemnizatorias fueron modificadas mediante el Real Decreto 37/2001, de 19 de enero, establece una serie de límites, concretamente de 300.000 euros. Así, el Real Decreto 1036/2017 reitera, en su artículo 26.c), la existencia de esos límites al exigir «*una póliza de seguro u otra garantía financiera que cubra la responsabilidad civil frente a terceros por los daños que puedan ocasionarse... según los límites de cobertura que se establecen en el Real Decreto 37/2001, de 19 de enero, por el que se actualiza la cuantía de las indemnizaciones por daños previstas en la Ley 48/1960, de 21 de julio, de Navegación Aérea, para las aeronaves de menos de 20 kg de masa máxima al despegue*». Hemos de hacer constar que ese límite es única y exclusivamente relativo al seguro, y no a la posible condena por daños, que se regirá por lo dispuesto en los artículos 1.902 y siguientes del Código civil.

Ante esta circunstancia, el problema que plantearon algunos autores a este respecto es la dificultad que entrañaría determinar los sujetos que estarían obligados a asegurarse<sup>260</sup>. Pero posteriormente, como decía, el propio Parlamento Europeo se posicionó de manera favorable a que no solo los productores contasen con ese seguro de responsabilidad civil obligatorio, sino que a ellos se sumasen los operadores de sistemas de inteligencia artificial, eso sí, limitándolos a aquellos que fuesen de alto riesgo, que tendrían que ser recogidos en un futuro anexo al Reglamento propuesto<sup>261</sup>. Esto no deja de tener sentido puesto que es el caso en el que la obligación de reparar nacerá de manera objetiva, y ha de asegurarse la reparación del mismo.

Lo mismo sucede con el informe de expertos ya mencionado sobre responsabilidad civil por los daños causados por la inteligencia artificial, que apuesta por la necesidad de que “*cuanto más frecuente o grave sea el daño potencial resultante de la tecnología digital emergente, y cuanto menos probable sea que el operador pueda indemnizar a las víctimas individualmente, más adecuado puede ser el seguro de responsabilidad civil obligatorio para tales riesgos*”. Esto nos abocaría, razonablemente, a la necesidad de establecer un seguro de responsabilidad civil obligatorio.

El riesgo que plantean algunos autores a este respecto, y que yo comparto plenamente, es que, con la existencia de un seguro, se tienda a limitar la responsabilidad al contratante de este, y no al verdadero causante del daño<sup>262</sup>.

Uno de los elementos más polémicos en lo referente al seguro de responsabilidad civil obligatorio es la existencia o no de límites indemnizatorios. Algunos autores sostienen que no se debería limitar ni los tipos de daños que deberían de ser reparados, ni la cuantía por la que se debería responder. Así SANTOS GONZÁLEZ sostiene que “*no se debe limitar el tipo o el alcance de los daños y perjuicios que puedan ser objeto de compensación, ni tampoco limitar*

---

260 Vid. GÓMEZ LIGÜERRE, C., y GARCÍA-MILCÓ, G.: “Liability for Artificial ... Op. cit., pág. 510

261 Vid. Parlamento Europeo (2020), *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*, pág. 12

262 Vid. TURNER, J.: *Robot Rules*, Palgrave Macmillan, 2019, pág. 75

*la naturaleza de dicha compensación, por el único motivo de que los daños y perjuicios hayan sido causados por robot y por tanto no por un humano. Se debe por tanto regular la responsabilidad objetiva contractual y extracontractual para adaptarla al nuevo paradigma*<sup>263</sup>.

La Unión Europea no ha mantenido esta postura en casos similares, como el de los daños producidos por los drones que, aunque a los que se refiere la legislación europea no estén dotados de inteligencia artificial, no dejan de ser robots. No obstante, el Parlamento Europeo, en su informe sobre normas de Derecho civil sobre robótica, sí se ha mostrado partidario de evitar cualquier limitación tanto en tipo de daño como en el alcance que los mismos han de tener. De este modo, el informe del Parlamento Europeo defiende que *“cualquier solución jurídica elegida en materia de responsabilidad de los robots y de la inteligencia artificial para los supuestos diferentes de los daños materiales no debería en modo alguno limitar el tipo o el alcance de los daños y perjuicios que puedan ser objeto de compensación, y tampoco debería limitar la naturaleza de dicha compensación, basándose únicamente en que los daños han sido causados por un agente no perteneciente a la especie humana”*<sup>264</sup>.

Como hemos señalado, la normativa que en estos momentos rige la responsabilidad de los daños provocados por los robots dotados de inteligencia artificial es la relativa a los daños producidos por productos defectuosos. Esa normativa actualmente establece tanto una limitación temporal para el ejercicio de la acción de reclamación por el daño producido como una limitación de la cuantía que se le puede exigir al autor del daño. El artículo 141 del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios fija un límite sobre la cuantía de la responsabilidad de productores o importadores que deriva de la facultad que concede la Directiva 374/85/CEE, en su artículo 16, a los Estados miembros de fijar tal límite<sup>265</sup>.

Es cierto que la Directiva contiene una regla de carácter ilimitado de la indemnización, ya que no se establece en ella ningún límite. No obstante, esta norma abre la posibilidad de que sean los propios Estados miembros los que, en virtud de sus tradiciones jurídicas, lo incluyan en su normativa nacional<sup>266</sup>, como así lo hizo el legislador español. La justificación a esta li-

263 Cfr. SÁNTOS GONZÁLEZ, M.J.: “Regulación legal... Op. cit, pág. 39

264 Cfr. Parlamento Europeo (2017), *Informe con recomendaciones...*, Op. cit. pág. 22

265 Dice el artículo 16 de la Directiva 374/85/CEE que *“cualquier Estado miembro podrá disponer que la responsabilidad global del productor por los daños que resulten de la muerte o lesiones corporales causados por artículos idénticos que presenten el mismo defecto, se limite a una cantidad que no podrá ser inferior a 70 millones de ECUS”*.

266 Así se desprende del considerando número 17 de la Directiva 374/85/CEE que, entendiendo *“que teniendo en cuenta las tradiciones jurídicas de la mayoría de los Estados miembros, no es conveniente fijar un límite financiero a la responsabilidad objetiva del productor; que, sin embargo, en tanto que existen tradiciones diferentes, parece posible admitir que un Estado miembro modifique el principio de la responsabilidad ilimitada estableciendo un límite para la responsabilidad global del productor por*

mitación la podemos encontrar en la idea de que la objetivación debe encontrar un límite y, a la misma vez, poder evitar cargas insufribles para los empresarios<sup>267</sup>.

En cambio, la propuesta de Reglamento recogida en el informe del Parlamento Europeo es favorable al establecimiento de un límite máximo por el que se deba indemnizar. No solo eso, sino que plantea que ese límite sea inferior que el recogido anteriormente, ya que “*el Reglamento solo se refiere al daño o perjuicio de una sola persona resultante de una única utilización de un sistema de IA, mientras que dicha Directiva se refiere a una serie de productos o, incluso, a una línea de productos con el mismo defecto.*” Los límites propuestos en el Reglamento son de dos millones de euros para los daños personales y de un millón de euros para los daños morales o patrimoniales<sup>268</sup>. Así, nos encontramos ante un pretendido equilibrio entre la protección de los perjudicados y los costes del producto y su puesta en circulación. En definitiva, se persigue una viabilidad real de que el daño sea indemnizado<sup>269</sup>.

Otro de los aspectos novedosos incluidos en el informe de expertos es la recomendación que se lleva a cabo para la implantación de un fondo de compensación. El Parlamento Europeo se ha mostrado contrario al establecimiento de este fondo propuesto en el informe de los expertos argumentando que “*un mecanismo de indemnización a escala de la Unión, financiado con fondos públicos, no es la manera adecuada de colmar posibles lagunas en materia de seguros*”<sup>270</sup>. Comparto la postura del legislativo comunitario porque esto gravaría a los contribuyentes europeos, evitando en cambio que se persiga y responsabilice al causante del daño con la energía necesaria para ello.

---

*los daños que resulten de la muerte o las lesiones corporales causadas por idénticos artículos con el mismo defecto, siempre que este límite se establezca lo suficientemente alto como para que queden asegurados la protección del consumidor y el correcto funcionamiento del mercado común”.*

267 VELA SÁNCHEZ, Antonio José, *Criterios de aplicación del régimen de responsabilidad civil por productos defectuosos*, Ed. Comares, 2004, pág. 157.

RODRÍGUEZ LLAMAS entiende que este límite se justifica por una necesidad de ponderar la cuantía indemnizatoria por razón de equidad ante un tipo de responsabilidad de la que no siempre se es culpable y una exigencia de técnica económica derivada de la necesidad de tener una cifra objetivada a efectos de una mejor ponderación y cálculo de coste de cobertura de un riesgo, medie o no la existencia de un seguro de esa posible responsabilidad civil. Cfr. RODRÍGUEZ LLAMAS, Susana, *Régimen de responsabilidad civil por productos defectuosos*, Ed. Aranzadi, 2002, págs. 142 y ss.

268 Art. 5 de la propuesta de Reglamento del Parlamento Europeo recogida en el *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*

269 Este tema lo traté con mayor profundidad en HERRERA DE LAS HERAS, R.: “Drones y responsabilidad civil”, *Derecho de los drones*, BARRIO ANDRÉS, M. (coord.), págs. 245-270

270 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, Recomendación núm. 25, pág. 10

Respecto al plazo de prescripción hemos de señalar que la Directiva 85/374 establecía un periodo de tres años a partir de la fecha en la que el demandante tuvo, o debió haber tenido, conocimiento del daño, del defecto y de la identidad del productor. Quizá se trate esta de la propuesta más rompedora y que más se diferencia con la actual. Por un lado, se establecen diferencias en lo que respecta al plazo dependiendo de si nos encontramos ante un daño personal o material o moral. Así el plazo de prescripción pasaría de los tres años mencionados a los treinta previstos para los daños personales, a contar desde que se produjo el daño. Para los daños materiales o morales el plazo sería de diez años para los casos habituales y de treinta para los daños provocados por un sistema de inteligencia artificial calificado como de alto riesgo<sup>271</sup>.

---

<sup>271</sup> Art. 7 del Reglamento propuesto por el Parlamento Europeo en el Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial

## BIBLIOGRAFÍA

- ALBADALEJO, M.: *Curso de Derecho Civil I* Ed. Barcelona, 2005
- APARICIO SALOM, J. y VIDAL LASO, M.: *Estudio sobre la protección de datos*, Ed. Aranzadi, 2019
- ARIAS DE RINCÓN, M.I.: “La calificación jurídica de las transmisiones de software en Internet”, en *Frónesis*, vol.14, núm.1, 2007
- BARR. A. y FEIGENBAUM. E: *The handbook of Artificial Intelligence Volumen I* Ed. William Kaufmann, 1981
- BARRIO ANDRÉS, M.: “Robótica, inteligencia artificial y Derecho”, en *Análisis del Real Instituto Elcano*, n°113, 2018
- BARRIO ANDRÉS, M.: *Derecho de los robots*, Ed. Wolters Kluwer, 2019
- BECK, U.: *La sociedad del riesgo. Hacia una nueva modernidad*. Ed. Paidós. Barcelona. 1998
- BERROCAL LANZAROT, I.: *Estudio jurídico-crítico sobre la Ley orgánica 3/2018, de 5 de diciembre de 2018 de protección de datos personales y garantía de los derechos digitales*, Ed. Reus, 2019
- BETANCOURT, F. *Derecho Romano Clásico*. Ed. Universidad de Sevilla, 2007
- BLÁZQUEZ AGUDO, E.M.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Ed. CISS, 2018
- BRUTAU, P.: *Fundamentos de Derecho Civil*. Ed. Bosch, Barcelona 1988
- BRYSON, J. J., DIAMANTIS, M.E. y GRANT, T.D.: “Of, for, and by the people: the legal lacuna of synthetic persons”, en *Artif Intell Law*, 2017
- BRYSON, J.J.: *La última década y el futuro del impacto de la IA en la sociedad*, Open Mind, 2017
- BRYSON, J.J.; DIAMANTIS, M.E.; GRANT, T.D. “Of, for, and by the People: The Legal Lacuna of Synthetic Persons.” *Artif Intell Law* 2017, n° 23
- BUCHANANT B.G. y HEADRICK, T.E.: “Some Speculation About Artificial Intelligence and Legal Reasoning”, en *Stanford Law Review*, Vol. 23, n°1, 1970
- CÁCERES, E.: “Inteligencia Artificial, Derecho y E-Justice”, en *Boletín Mexicano de Derecho Comparado*, n° 116, 2006

- CANALS AMETLLER, D.: “El proceso normativo ante el avance tecnológico y la transformación digital (Inteligencia artificial, redes sociales y datos masivos)”, en *Revista General de Derecho Administrativo*, n° 50, 2019
- CASADESUS RIPOLL, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, en *Revista de la Facultad de Derecho de México*, núm. 278, 2020, pág. 359
- CASTÁN TOBEÑAS, J.: *Derecho Civil Español Común y Foral*; Tomo II Vol. I, Ed. REUS, 1995
- Cfr. DE CASTRO Y BRAVO, F.: *Derecho Civil de España*, Tomo II, Ed. Aranzadi 2008
- CORVALÁN, J.G.: “Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia”, en *Revista de Investigações Constitucionais*, Vo.5, n°1, 2018
- COSSIO CORRAL, A.: “Hacia un nuevo concepto de la persona jurídica”, en *Anuario de Derecho Civil*, 1954
- COTINO HUESO, L.: “Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales”, en *Dilemata*, núm. 24, 2017
- COTINO HUESO, L.: “Inteligencia Artificial y vigilancia digital contra el Covid-19 y contra la privacidad. El diablo está en los detalles”, en *Boletín Español de Estudios Estratégicos*, 23 de abril de 2020
- DE MONTALVO JÄÄSKELÄINEN, F.: “Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del big data”, en *Revista de Derecho Político*, núm. 106, 2019
- DÍAZ ALABART, S.: “Robots y responsabilidad civil”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018
- DYSCHKANT, A.: “Legal Personhood: How We Are Getting It Wrong”, en *University of Illinois Law Review*, n° 36
- EBERS, M. “La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?”, en *Indret Revista para el Análisis del Derecho*, núm. 3, 2016
- ERCILLA GARCÍA, J.: “Aproximación a una Personalidad Jurídica Específica para los robots”, en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n°47, 2018
- FERNÁNDEZ HERNÁNDEZ, C.: “La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución”, en *Derecho digital e innovación*, n°5, 2020
- FERRARA, F.: *Teoría de las Personas Jurídicas*, Ed. Comares, 2006
- GARCÍA-PRIETO CUESTA, J.: “¿Qué es un robot?”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluwer
- GARDNER, H: *Frames of Mind. The Theory of Multiple Intelligences*, Ed. Basic Books

- GIUFFRIDA, I.: “Liability for AI decisión-making: Some legal and ethical considerations.”, en *Fordham Law Review*, Vol. 88, núm. 2
- GÓMEZ LIGÜERRE, C., y GARCÍA-MILCÓ, G.: “Liability for Artificial Intelligence and other emerging technologies”, en *Revista para el análisis del Derecho*, núm. 1, 2020
- CASADESUS RIPOLL, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, en *Revista de la Facultad de Derecho de México*, núm. 278, 2020
- GARCÍA-PRIETO CUESTA, J.: “¿Qué es un robot?”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluver
- GÓMEZ SALADO, M.A.: “Robótica, empleo y seguridad social. La cotización de los robots para salvar el estado del bienestar”, en *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Vol. 6, nº3, 2018
- GÓMEZ-RIESCO TABERNEIRO DE PAZ, J.: “Los robots y la responsabilidad civil extracontractual”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluver
- GUARDIOLA SALMERÓN, M.: “Robótica e inteligencia artificial: nuevos desafíos jurídicos”, en *Law & Trends*, julio 2016
- GUNTHER, J., MUNCH, F., BECK, LOFFLER, S. y LABRUTO, R., “Issues of privacy and electronic personhood in robotics. Proceedings”, *IEEE International Workshop on Robot and Human Interactive Communication*, 2012
- HERNÁNDEZ GIMENEZ, M.: “Inteligencia Artificial y Derecho Penal”, en *Actualidad jurídica iberoamericana*, nº 10 bis, 2019
- HERRERA DE LAS HERAS, R.: “Drones y responsabilidad civil”, *Derecho de los drones*, BARRIO ANDRÉS, M. (coord.)
- HERRERA DE LAS HERAS, R.: *Políticas jurídicas para el menor*, SAINZ-CANTERO CAPARRÓS, M.B. (Dir.), Ed. Comares 2010, págs. 75 y ss.
- HIDALGO PÉREZ, A.: “Robots e impuestos”, en *ICE, Revista de Economía*, núm. 917, 2020
- HOCHÉL, M y GÓMEZ MILÁN, E: *La inteligencia*, 2012
- JIMÉNEZ LIÉBANA, D.: *Responsabilidad civil: daños causados por productos defectuosos*, Ed. McGraw-Hill, 1998
- KINGSTON, J.: *Artificial Intelligence and Legal Liability, International Conference on Innovative Techniques and Applications of Artificial Intelligence*, 2016
- KOKKINAKIS, D.: “Complementary Methods for De-identifying Sensitive Data with a focus on Clinical Discourse”, en *Procesamiento del Lenguaje Natural*, núm. 45, 2010
- KROES, N. (2013), accesible en <https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-011289&language=EN>
- KURKI, A.J. y PIETRZYKOWSKI, T.: *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Ed. Springer, 2017

- LACRUZ MANTECÓN, M.L.: “Potencialidades de los robots y capacidades de las personas”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018
- LEAN LAU, P: “The Extension of Legal Personhood in Artificial Intelligence”, en *Revista de Bioética y Derecho*, n° 46
- MARTÍNEZ MARTÍNEZ, R.: “Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo”, en *Revista Catalana de Dret Públic*, núm. 58, 2019
- MATURO SERNA, A.: “Inteligencia artificial y privacidad: un encaje problemático.”, en *La Ley*, núm. 2, 2019
- McCARTHY, J., MINSKY, M.L., ROCHESTER, N., SHANNON, C.E., *A proposal for the Dartmouth summer research Project on artificial intelligence*, 1956
- MIRALLES LÓPEZ, R.: “Desvinculando datos personales: Seudonimización, Desidentificación y Anonimización”, en *Revista de la Sociedad Española de Informática y Salud*, núm. 122, 2017
- MIRÓ LLINARES, F.: “Inteligencia artificial y justicia penal: Más allá de los resultados lesivos causados por robots”, en *Revista de Derecho Penal y Criminología*, 3º Época, n.º 20, 2018
- NAVARRETE B, J.: “El origen de la responsabilidad civil objetiva en el derecho aéreo”, en *Revista Chilena de Derecho*, núm. 1, 1978
- NAVEJANS y SHARKEY han mantenido esta postura en distintas ocasiones. Recogido en “Europe divided over robot ‘personhood’”, *Político*, 2018. Accesible en <https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood/>
- O’CALLAGHAN MUÑOZ, X.: *Código Civil Comentado y con Jurisprudencia*. Ed. La Ley, Madrid 2008
- O’CALLAGHAN MUÑOZ, X.: *Compendio de Derecho Civil*. Tomo I Parte General. Ed. Revista de Derecho Privado. 1997
- PAGALLO, U.: “Vital, Sophia, and Co.—The Quest for the Legal Personhood of Robots”, en *Information* n° 9
- PALMERINI, E. (2014), *The RoboLaw Project: A European perspective on the ethical and legal implications of social robots*
- PALMERINI, E.: “Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea”, en *Revista de Derecho Privado*, n°32, 2017
- PAVÓN PÉREZ, J.A.: “La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales”, en *Anuario de la Facultad de Derecho. Universidad de Extremadura*, n° 19, 2002
- PAZOS, A., PEDREIRA, N., RABUÑAL, J.R. y PEREIRA, J.: “Inteligencia Artificial y computación avanzada”, *Inteligencia Artificial y computación avanzada*,

ROMERO, J.J., DAFONTE, C., GÓMEZ, A., PENOUSAL, F.J. (EDS.) eD. Fundación Alfredo Brañas, 2007

- PEDREÑO MUÑOZ, A. y MORENO IZQUIERDO, L.: “El impacto económico de la Inteligencia Artificial”, *Big Data e Inteligencia Artificial. Una visión económica y legal de estas herramientas disruptivas*, Ed. Universidad de Valencia, 2018
- PÉREZ LUÑO, A. E.: *Cibernética, Informática y Derecho. Un análisis metodológico*, Ed. Publicaciones del Real Colegio de España, 1976
- PÉREZ SANZ, C.: “Aspectos legales del Big Data”, en *Revista de estadística y sociedad*, núm. 68, 2016
- PÉREZ, C.: “Inteligencia Artificial y Educación”, en *Anales de la Pedagogía*, n°7, 1989
- PETIT, M.: “Por una crítica de la razón algorítmica. Estado de la cuestión sobre la inteligencia artificial, su influencia en la política y su regulación”, en *Quaderns del CAC*, n°44, 2018
- PIÑAR, J.L. Privacidad en estado de alarma y normal aplicación de la Ley [Blog]. (2020) accesible en <https://hayderecho.expansion.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/>
- PLAZA PENADÉS, J.: “Aspectos legales de la Inteligencia Artificial y el Big Data”, *Big Data e Inteligencia Artificial. Una visión económica y legal de estas herramientas disruptivas*, Ed. Universidad de Valencia, 2018
- PUGLIANO, J.: *The Robots are Coming : A Human's Survival Guide to Profiting in the Age of Automation*, Ed. Ulysses Press, 2017
- REBOLLO DELGADO, L.: *Protección de datos personales*, Ed. Dykinson, 2018
- RICH, E. y KNIGHT, K.: *Inteligencia Artificial* Mc Graw Hill 1994
- RUESTRA HERRERA, E.: *Privacidad en el diseño de la inteligencia artificial*, Editado por Riestra Abogados, 2017
- RODRÍGUEZ CARRIÓN, J. L.: *La responsabilidad civil por los daños causados por productos defectuosos*. Ediciones Revista General de Derecho. Valencia, 2000
- RODRÍGUEZ LLAMAS, S.: *Régimen de responsabilidad civil por productos defectuosos*, Ed. Aranzadi, 2002, págs. 142 y ss.
- ROGEL VIDE, C.: “Robots y personas”, *Los robots y el Derecho*, ROGEL VIDE, C. (Coord.), Ed. Reus, 2018
- SAIF, I. y AMMANATH, B.: “Trustworthy AI is a framework to help manage unique risk” en *MIT Technology Review*, 25 de marzo 2020
- SÁNCHEZ DEL CAMPO REDONDET, A.: “Inteligencia artificial y privacidad”, *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPD-GDD*, LÓPEZ CALVO, J. (Coord.), Ed. Bosch, 2019
- SÁNCHEZ DEL CAMPO REDONDET, A.: “Europa quiere regular a los robots”, en *Diario la Ley*, n°4, 2017

- SÁNCHEZ ZAPLANA, A.: “Breve introducción a la Inteligencia Artificial para todos los públicos”, en *El Consultor de los Ayuntamientos*, n°10, octubre 2019
- SÁNCHEZ-URAN AZAÑA, M.Y., y GRAU RUIZ, M.A.: *El impacto de la robótica, en especial la robótica inclusiva, en el trabajo: Aspectos jurídico-laborales y fiscales*. Ponencia presentada al Congreso Internacional sobre Innovación tecnológica y futuro del trabajo, Santiago de Compostela, 5 y 6 de abril de 2018
- SANTOS GONZÁLEZ, M.J.: “Regulación legal de la robótica y la inteligencia artificial: Retos de futuro”, en *Revista Jurídica de la Universidad de León*, n° 4, 2017
- SANTOS SÁNCHEZ, D. J., *Tratamientos Asociados Al Contexto De La Epidemia: Principios De Protección De Datos, Legitimación Y Actores Intervinientes*, conferencia durante el curso “La protección de datos personales en el marco de la epidemia COVID-19”, Santander, 2020
- SARRIÓN ESTEVE, J.: “The problem of the consent for the processing of health data, particularly for biomedical research purposes, from the perspective of fundamental rights protection in the Digital Era”, en *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, núm. 48, 2018
- SCHNEIDER, K. (2020). Judge Recognizes Two Chimpanzees as Legal Persons, Grants them Writ of Habeas Corpus (Blog). Accesible en <https://www.nonhumanrights.org/blog/judge-recognizes-two-chimpanzees-as-legal-persons-grants-them-writ-of-habeas-corporus/>
- SEGURA ALASTRUÉ, M.: “Los robots en el Derecho financiero y tributario”, *Derecho de los robots*, BARRIO ANDRÉS, M. (Dir.), Ed. Wolters Kluwer
- SERRANO VILLAFAÑE, E., “Funciones del Derecho en la sociedad cambiante de nuestros días”, en *Anuario de Filosofía del derecho*, n°17, 1974
- SHRAFIAN, H. “AIonAI: A Humanitarian Law of Artificial Intelligence and Robotics.”, en *Science and Engineering Ethics*, 2015
- SOBRINO GARCÍA, I.: “Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos”, en *Revista de Derecho UNED*, núm. 25, 2019
- SOLAIMAN, S.M.: “Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy”, en *Artif Intell Law*, 2017
- TENA R.: “Hacia un salto evolutivo en el Derecho civil: de la justicia conmutativa a la disuasión”, en *El Notario*, n. 90, 2020
- TIMÓN HERRERO, M.: “Protección de datos de carácter personal y crisis sanitaria (Covid 19)”, en *elderecho.com*, 7 de agosto de 2020
- TURNER, J.: *Robot Rules*, Palgrave Macmillan, 2019
- VALENTE, L.A.: “La persona electrónica”, en *Anales de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de la Plata*, Vol. 16, núm. 49, 2019
- VELA SÁNCHEZ, Antonio José, *Criterios de aplicación del régimen de responsabilidad civil por productos defectuosos*, Ed. Comares, 2004

- WAMSLEY, L. (2020). Stanford Apologizes After Vaccine Allocation Leaves Out Nearly All Medical Residents. *NPR*.
- WEGMANN STOCKEBRAND, A.: “Sobre la noción de contrato en las instituciones de Gayo”, en *Revista de Derecho Privado*, n°34, 2018
- WRITZ, K.: “Cómo hacen Netflix y Spotify para saber lo que te gusta (sí, con inteligencia artificial)”, en *Entrepreneur*, octubre de 2018
- YU, E.: Singapore police can access COVID-19 contact tracing data for criminal investigations. *Zdnet*. 4 de enero 2021



## GRACIAS POR CONFIAR EN NUESTRAS PUBLICACIONES

Al comprar este libro le damos la posibilidad de consultar gratuitamente la versión ebook.

### Cómo acceder al ebook:

- ☞ **Entre en nuestra página web**, sección Acceso ebook  
([www.dykinson.com/acceso\\_ebook](http://www.dykinson.com/acceso_ebook))
- ☞ **Rellene el formulario** que encontrará insertando el código de acceso que le facilitamos a continuación así como los datos con los que quiere consultar el libro en el futuro (correo electrónico y contraseña de acceso).
- ☞ Si ya es **cliente registrado**, deberá introducir su **correo electrónico y contraseña habitual**.
- ☞ Una vez registrado, **acceda a la sección Mis e-books de su cuenta de cliente**, donde encontrará la versión electrónica de esta obra ya desbloqueada para su uso.
- ☞ Para consultar el libro en el futuro, ya sólo es necesario que se identifique en nuestra web con su correo electrónico y su contraseña, y que se dirija a la sección Mis ebooks de su cuenta de cliente.



### CÓDIGO DE ACCESO

Rasque para ver el código

Nota importante: Sólo está permitido el uso individual y privado de este código de acceso. Está prohibida la puesta a disposición de esta obra a una comunidad de usuarios.

**MANTÉNGASE INFORMADO  
DE LAS NUEVAS PUBLICACIONES**

**Suscríbase gratis  
al boletín informativo  
[www.dykinson.com](http://www.dykinson.com)**

**Y benefíciense de nuestras ofertas semanales**