

LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL EN LA NUEVA ERA DE LA REVOLUCIÓN INDUSTRIAL 4.0

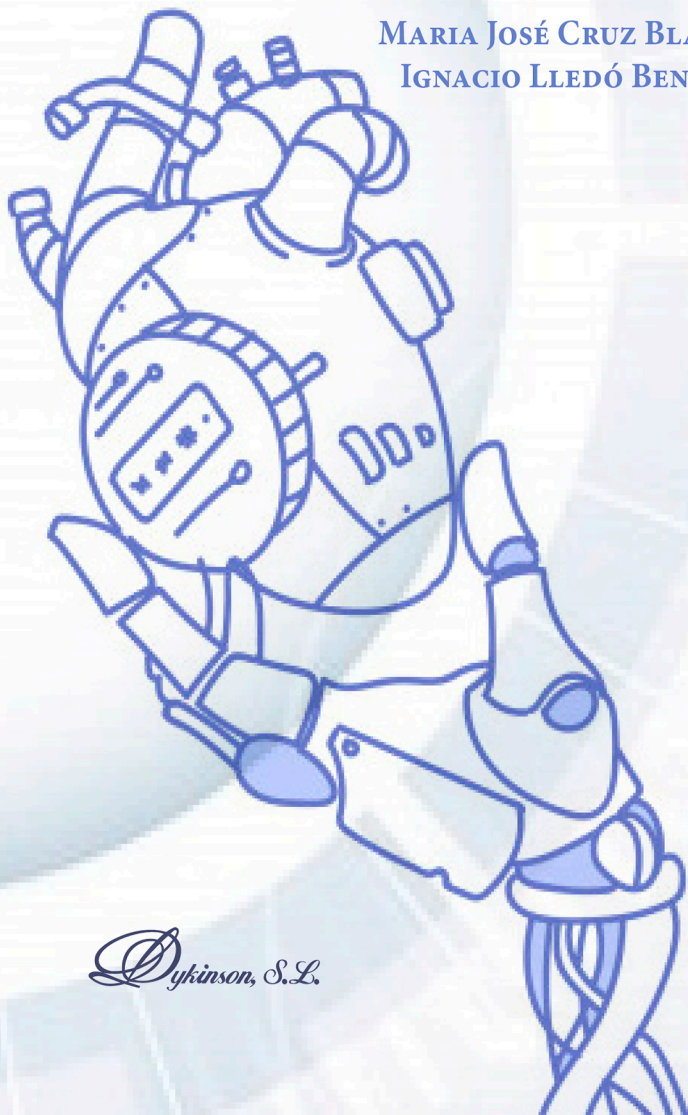
(Los desafíos jurídicos, éticos y tecnológicos
de los robots inteligentes)

Directores

FRANCISCO LLEDÓ YAGÜE
IGNACIO BENITEZ ORTÚZAR
OSCAR MONJE BALMASEDA

Coordinadores

MARIA JOSÉ CRUZ BLANCA
IGNACIO LLEDÓ BENITO



Dykinson, S.L.

Colección
IA, Robots, y Bioderecho

LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL
EN LA NUEVA ERA DE LA REVOLUCIÓN INDUSTRIAL 4.0
(Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes)

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

Coordinadores

M^a JOSÉ CRUZ BLANCA
Profesora 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'ELLOSO
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

LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL EN
LA NUEVA ERA DE LA REVOLUCIÓN INDUSTRIAL 4.0
(Los desafíos jurídicos, éticos
y tecnológicos de los robots inteligentes)

DIRECTORES

FRANCISCO LLEDÓ YAGÜE
IGNACIO BENITEZ ORTÚZAR
OSCAR MONJE BALMASEDA

COORDINADORES

MARIA JOSÉ CRUZ BLANCA
IGNACIO LLEDÓ BENITO

 *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 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

El presente trabajo se ha realizado financiado por el Proyecto de I+D+i
DERECHO Y MEDICINA: DESAFIOS TECNOLOGICOS Y CIENTIFICOS
(DEMETYC) PID2019104868RA-I00 / AEI /10.13039/501100011033.



© Copyright by
Los autores
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
<http://www.dykinson.es>
<http://www.dykinson.com>

ISBN: 978-84-1324-802-8
Depósito Legal: M-20511-2021

ISBN electrónico: 978-84-1377-661-3

Preimpresión por:
Besing Servicios Gráficos S.L.
e-mail: besingsg@gmail.com

Índice

INTRODUCCIÓN. “LA DISRUPCIÓN DISTÓPICA DE LA MÁQUINA PENSANTE Y LA SUPERACIÓN DEL HOMBRE ÓPTIMO”	15
FRANCISCO LLEDÓ YAGÜE E IGNACIO BENÍTEZ ORTÚZAR	
REALIDADES Y DISRUPCIONES EN TORNO AL ROBOT INTELIGENTE (EL FUTURO DEL HOMBRE QUEBRADIZO)*	25
FRANCISCO LLEDÓ YAGÜE	
1. El enfoque de la cuestión: la vida inteligente, el avance de la robótica y la inteligencia artificial	25
2. Érase una vez... del autómeta del medievo al cibor del siglo XXI	29
3. Algunas reflexiones en la consideración evolutiva del robots inteligente <i>versus</i> persona.....	54
Conclusiones	70
Bibliografía.....	70
CIBERDELITOS. LA IMPLEMENTACIÓN EN EL ORDENAMIENTO INTERNO DE LOS ACUERDOS INTERNACIONALES EN MATERIA DE CIBERDELINCUENCIA.....	79
IGNACIO F. BENÍTEZ ORTUZAR	
1. Introducción. Acerca de la ciberdelincuencia.....	79
2. El convenio sobre ciberdelincuencia del Consejo de Europa	84
3. Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos.....	87
4. Delitos informáticos	105
5. Delitos relacionados con el contenido.....	116
6. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.....	121
7. Otras actividades delictivas relacionadas con las tecnologías de la información y la comunicación.....	124
Conclusion	126
Bibliografía.....	127

LA SEXUALIZACIÓN DE LAS TECNOLOGÍAS. LOS DELITOS DE CIBER-EMBAUCAMIENTO CON FINES SEXUALES DEL ART. 183 TER DEL CÓDIGO PENAL	129
MARÍA JOSÉ CRUZ BLANCA	
1. Introducción.....	129
2. Las formas de ciberdelincuencia sexual sobre los menores de edad ...	131
3. Los menores como posibles autores de los delitos de ciberdelincuencia sexual y su tratamiento en aplicación de la Ley Orgánica 5/2000, Reguladora de la Responsabilidad Penal de los menores	141
4. Un apunte final	147
BIBLIOGRAFÍA.....	148
VISIÓN DEL DERECHO PENAL EN RELACIÓN CON LA ROBÓTICA, IA Y LA CIBERDELINCUENCIA	149
IGNACIO LLEDÓ BENITO	
1. El derecho y el ciberespacio	149
2. Ciberseguridad versus ciberdelincuencia.....	153
3. El impacto de la robótica. La inteligencia artificial y la responsabilidad penal en los robots inteligentes	156
Conclusiones	193
Bibliografía.....	194
LA RESPONSABILIDAD CIVIL EN TIEMPOS DE LA IA Y LOS ROBOTS	197
IÑIGO A. NAVARRO MENDIZABAL	
1. Contexto.....	197
2. ¿Qué es la IA y qué son los robots?	207
3. La necesidad de principios éticos y de una normativa europea en la materia de RC de la IA y los robots	211
4. Hay elementos de la posible RC de la IA y de los robots que no encajan en la RC que tenemos	217
5. Los posibles responsables: la RC propia de los robots	223
6. Los posibles responsables: la RC del fabricante, del formador, del usuario, del poseedor O del que se sirve del robot	228
7. Conclusiones	236
Abreviaturas	236
Bibliografía.....	237

**RESPONSABILIDAD CIVIL,
ROBÓTICA E INTELIGENCIA ARTIFICIAL 239**

OSCAR MONJE BALMASEDA

1. La ausencia de un marco normativo adaptado a la nueva realidad y la necesaria revisión legislativa. De la “personalidad electrónica” a la búsqueda de soluciones concretas 239
2. Aspectos a considerar en la nueva normativa. El sistema de responsabilidad civil y la protección de datos. 246
3. Las previsiones de la Unión Europea en relación con la responsabilidad civil de los robots y los sistemas de inteligencia artificial 250
4. Principales retos a abordar en relación con la responsabilidad civil de los robots. Problemas y soluciones. 256
5. Conclusiones 260
6. Bibliografía..... 262

**PANORAMA LEGISLATIVO DE LA INTELIGENCIA ARTIFICIAL EN LA
UNIÓN EUROPEA 265**

VANESSA GARCÍA HERRERA

1. Necesidad de un concepto flexible y generalmente aceptado de inteligencia artificial como prólogo de su reglamentación 265
 2. El auge de la inteligencia artificial: la cuarta revolución humana..... 266
 3. La regulación de la inteligencia artificial: actualización del marco jurídico europeo y de los marcos jurídicos nacionales versus creación de instrumentos jurídicos nuevos y específicos..... 273
 4. Conclusiones 296
- Bibliografía..... 300

**LAS DIFERENTES FORMAS EN QUE SE MANIFIESTA
LA INTELIGENCIA ARTIFICIAL EN LA SOCIEDAD
Y EN LA ECONOMÍA 303**

BLANCA BALLESTER CASANELLA

1. Introducción 303
2. La inteligencia artificial y su impacto en la sociedad actual..... 308
3. La imputación de responsabilidad civil en materia de inteligencia artificial 313
4. La implantación de la tecnología disruptiva en las empresas..... 319

5.	El impacto de las nuevas tecnologías en el ámbito laboral: Especial referencia a la sentencia del Juzgado de lo Social número 10 de las Palmas de Gran Canaria de 23 de septiembre de 2019.....	323
6.	Conclusiones	328
	Bibliografía.....	330
LA RESPONSABILIDAD EXTRA CONTRACTUAL DEL CÓDIGO CIVIL Y LOS VEHÍCULOS AUTOMATIZADOS		333
ALEJANDRO ZORNOZA SOMOLINOS		
1.	Introducción.....	333
2.	La automatización de la conducción. El estándar J3016 SAE.....	334
3.	La responsabilidad civil automovilística y el seguro obligatorio de automóviles	336
4.	Regímenes de responsabilidad extracontractual en el Código civil	341
5.	Conclusiones	355
6.	Bibliografía.....	356
ROBÓTICA Y PROTECCIÓN DE DATOS: ADECUACIÓN A UN DESPACHO DE ABOGADOS		359
JOSÉ RICARDO PARDO GATO		
1.	Desde la aprobación de la “ley de internet” hasta los nuevos retos tecnológicos: inteligencia artificial, machine learning, chatbots, bitcoin y blockchain, big data... ..	360
2.	Ciberseguridad y secreto profesional: la utilización del sistema lexnet y la autoridad de certificación de la abogacía	367
3.	Protección de datos de carácter personal.....	372
4.	Adaptación de un despacho de abogados a la normativa sobre protección de datos: impacto normativo comparado (a modo de informe técnico).....	382
5.	Conclusiones generales	435
	Normativa y otras fuentes.....	441
	Jurisprudencia.....	443
	Bibliografía.....	444

¿ES NECESARIO UN MARCO ÉTICO PARA GUIAR EL DESARROLLO Y USO DE LA INTELIGENCIA ARTIFICIAL EN LAS ORGANIZACIONES? ... 449

MARÍA CUMBRERAS
PEDRO LÓPEZ

1.	Introducción.....	449
2.	Marco jurídico y político europeo de la ia: hacia una IA fiable.....	461
3.	Un marco ético para el desarrollo y el uso de la IA.....	474
4.	El cumplimiento y el buen gobierno: la exigencia obligada de un marco ético empresarial para el desarrollo y uso de la IA	478
5.	Conclusiones	483
	Bibliografía.....	484

DERECHO CONSTITUCIONAL E INTELIGENCIA ARTIFICIAL..... 487

MARÍA MERCEDES SERRANO PÉREZ
CELIA FERNÁNDEZ ALLER

1.	Introducción.....	488
2.	La inteligencia artificial desde un enfoque constitucional.....	493
3.	La regulación de la unión europea sobre inteligencia artificial. Marco normativo	495
4.	El estado social y la inteligencia artificial	504
5.	El estado de derecho y la inteligencia artificial: principio de seguridad jurídica e interdicción de la arbitrariedad. Principio de legalidad	511
6.	Interrelación entre inteligencia artificial y derechos fundamentales ..	515
7.	Surgimiento de nuevos derechos.....	537
8.	Conclusiones	542
	Bibliografía.....	544

CAMINOS HACIA LA SUPERINTELIGENCIA (EMULACIÓN DE CEREBRO COMPLETO) 545

HUMBERTO BUSTINCE SOLA

1.	La evolución del concepto de inteligencia artificial	545
2.	Los problemas que trata la inteligencia artificial.....	547
3.	Paradigmas de la inteligencia artificial.....	549
4.	Inteligencia computacional o soft computing.....	552

5.	El problema de la inteligencia artificial fuerte	554
6.	Breve repaso de la historia reciente de la inteligencia artificial	556
7.	Aprendizaje profundo. ¿Hacia el supercerebro?	559
8.	La clave de la inteligencia artificial: datos y ciencia de datos	565
9.	¿Debemos temer la inteligencia artificial?.....	568
10.	Conclusiones	569
	Referencias.....	569
 VOLUNTAD SUPERINTELIGENTE EFECTOS DE LOS AVANCES DE HARDWARE		573
JOSÉ LUIS LIEBANA CÁRDENAS		
 AVANCES CIENTÍFICO-TECNOLÓGICOS EN INTELIGENCIA ARTIFICIAL RESPONSABLE		593
JAVIER ANDREU-PEREZ, LUIS MARTÍNEZ, ANA R ANDREU-PEREZ, DEEPAK SHARMA, PRASHANT GUPTA J. ANDREU-PEREZ, L. MARTÍNEZ, A. R ANDREU-PEREZ, D. SHARMA, P. GUPTA		
1.	Introducción.....	593
2.	El aprendizaje automático.....	594
3.	Hacia una ia adaptada para convivir en la sociedad de forma respon- sable	595
4.	Inteligencia artificial interpretable (XAI).....	597
5.	Lógica difusa	598
6.	Computación con palabras	599
7.	Análisis documental de las publicaciones inteligencia artificial inter- pretable.....	600
8.	El sesgo en la inteligencia artificial.....	605
9.	Preservación de la privacidad en la IA	606
10.	La inteligencia artificial social y afectiva	607
11.	Conclusión	611
12.	Referencias.....	612

¿POR QUÉ DEBERÍA CONFIAR EN TI (MÁQUINA)?	617
LUIS MAGDALENA LAYOS	
1. Introducción	617
2. ¿Seremos la última generación más inteligente que las máquinas?.....	618
3. ¿Hacia dónde se dirige la inteligencia artificial?	619
4. ¿Tienen voluntad las máquinas?	621
5. ¿Pueden tener sentimientos?.....	622
6. ¿Son ecuanímes las máquinas?	624
7. ¿Qué guía sus decisiones, algún tipo de ética <i>robótica</i> ?	626
8. ¿Podemos fiarnos de una máquina que sea más inteligente que nosotros?.....	631
9. ¿Por qué debería fiarme de ti (máquina)?	632
10. Inteligencia artificial explicable	635
11. Conclusiones	640
Bibliografía.....	641
PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL.....	643
RAMÓN HERRERA DE LAS HERAS	
1. Concepto de inteligencia artificial y de robot.....	643
2. Concepto del Derecho a la protección de datos	645
3. Privacidad, protección de datos e inteligencia artificial	652
4. Inteligencia Artificial y protección de datos en tiempos de pandemia	660
5. Conclusiones	667
Bibliografía.....	667

PANORAMA LEGISLATIVO DE LA INTELIGENCIA ARTIFICIAL EN LA UNIÓN EUROPEA

VANESSA GARCÍA HERRERA
Prof. Titular de Universidad I URJC

Sumario: 1. Necesidad de un concepto flexible y generalmente aceptado de inteligencia artificial como prólogo de su reglamentación. 2. El auge de la inteligencia artificial: la cuarta revolución humana. 3. La regulación de la inteligencia artificial: actualización del marco jurídico europeo y de los marcos jurídicos nacionales versus creación de instrumentos jurídicos nuevos y específicos. 3.1. El eterno debate. 3.2. Estado actual de la cuestión. 4 Conclusiones. Bibliografía

1. NECESIDAD DE UN CONCEPTO FLEXIBLE Y GENERALMENTE ACEPTADO DE INTELIGENCIA ARTIFICIAL COMO PRÓLOGO DE SU REGLAMENTACIÓN

No existe, a fecha de hoy, un concepto preciso y generalmente aceptado de inteligencia artificial. Esta carencia representa un obstáculo para la consecución de una reglamentación adecuada, eficiente, transparente y coherente de la materia. Presupuesto *sine qua non* de toda regulación es la determinación de su ámbito de aplicación; de ahí que el tema conceptual no sea una cuestión baladí.

La Comisión Europea¹ ofreció una primera definición en su *Comunicación sobre Inteligencia Artificial para Europa*², estableciendo que el término «se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción -con cierto grado de autonomía- con el fin de alcanzar objetivos específicos». Aclaraba, a renglón seguido, que los sistemas basados en la inteligencia artificial pueden consistir simplemente en un programa informático (por ejemplo, asistentes de voz, programas de análisis de imágenes, motores de búsqueda y sistemas de reconocimiento facial o de voz) o estar incorporados en disposi-

¹ La Comisión Europea ha reiterado la necesidad de crear una definición de inteligencia artificial generalmente aceptada que sea flexible y no lastre u obstaculice la innovación y el desarrollo.

² COM(2018)237 final, p. 1.

tivos de hardware (por ejemplo, robots avanzados, automóviles autónomos, drones y aplicaciones del internet de las cosas).

Esta definición fue posteriormente perfeccionada por el Grupo de Expertos de Alto Nivel en Inteligencia artificial³, que consideró que los sistemas de inteligencia artificial «son programas informáticos (y posiblemente también equipos informáticos) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados y no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado»⁴.

En este contexto de ausencia de un concepto uniforme, la Comisión Europea insta a que, en los instrumentos jurídicos que puedan elaborarse sobre la materia, la definición que se ofrezca de inteligencia artificial sea lo suficientemente flexible como para adaptarse al progreso técnico al tiempo que mantenga un nivel de precisión adecuado para ofrecer la seguridad jurídica necesaria⁵. Y precisamente siguiendo esta consideración, el Parlamento Europeo ha definido recientemente los sistemas de inteligencia artificial como «todo 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».

2. EL AUGE DE LA INTELIGENCIA ARTIFICIAL: LA CUARTA REVOLUCIÓN HUMANA

El término inteligencia artificial se acuñó por primera vez en 1956 por el informático John Patrick McCarthy (con la ayuda de Marvin Minsky y Claude Shannon) en la Conferencia de Dartmouth (evento germen de la inteligencia artificial como esfera), quien la definió como la ciencia e ingeniería de “hacer máquinas inteligentes,

³ El Grupo de Expertos de Alto Nivel en Inteligencia Artificial (AI HLEG) fue creado por la Comisión Europea en junio de 2008, está integrado por 52 expertos, entre ellos representantes de la academia, de la sociedad civil y de la industria. Su objetivo general es apoyar la implementación de la *Estrategia Europea de Inteligencia Artificial*, lo cual incluye la elaboración de recomendaciones sobre el desarrollo de políticas relacionadas con el futuro y sobre cuestiones éticas, legales y sociales relacionadas con la inteligencia artificial, incluidos los desafíos socioeconómicos (<https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>).

⁴ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>.

⁵ *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica* de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo de 19 de febrero de 2020 (COM(2020)64 final y 65 final, p. 20).

especialmente programas de cálculo inteligentes”; no concebía la inteligencia artificial como la imitación del comportamiento humano por parte de las máquinas o las computadoras, sino como aquella inteligencia que puede replicarlo⁶. Sus bases se establecieron por ALAN TURING en 1950 en su estudio *Computing Machinery and Intelligence* (Máquinas de Computación e Inteligencia), en el que sugirió sustituir la pregunta ¿pueden pensar las máquinas?, planteada en 1637 por el filósofo y matemático René Descartes, por el interrogante ¿pueden las máquinas hacer lo que nosotros (como entidades pensantes) podemos hacer? y presentó, a tal efecto, la *prueba o test de turing*⁷.

Hasta la década de los 90 el concepto evolucionó con cierta lentitud. Por citar algunas aplicaciones prácticas, en 1957 Frank Rosenblatt diseñó la primera red neuronal artificial, en 1966 Joseph Weizenbaum desarrolló el primer chatbot (ELIZA⁸) en el Massachusetts Institute of Technology (MIT), en 1973 se desarrolló en SRI el primer lenguaje de programación para robots con la denominación WAVE, en 1979 la máquina BKG 9.8 logró derrotar a Luigi Villa, campeón de backgammon, en este juego, también en ese mismo año Ernst Dickmanns trabajó en su modelo de visión artificial y tres años más tarde, en 1982, consiguió que un vehículo eléctrico se moviera a derecha y a izquierda, fenómeno que se erigió como nacimiento de los vehículos autónomos.

En 1990 la inteligencia artificial coge impulso e inicia su edad de oro, que encuentra su fundamento principal en el repentino desarrollo de la tecnología, que afectaba directamente a las industrias. Las empresas comenzaron en aquel entonces a invertir en tecnología y surgió el llamado “mundo digital”, en el que se produjo una mejora de la capacidad de procesamiento y análisis de ingentes cantidades de datos. A comienzos de esta década, el experto en inteligencia artificial Kai-Fu Lee creó a CASPER, el primer sistema de reconocimiento de voz que presentó Apple en 1992 y que puede considerarse como el antepasado de la tecnología de análisis del habla actual, en 1994 varios vehículos autónomos recorrieron unos 1000 kilómetros de autopistas en los alrededores de París y en 1997 la multinacional IBM presentó a DEEP BLUE, un ordenador provisto de inteligencia artificial capaz de ganar una partida de

⁶ De acuerdo con esta concepción la mayoría de las aplicaciones de inteligencia artificial actuales no podrían ser consideradas como tales; *vide* ORTIZ HERNÁNDEZ, S., GARROS FONT, I. y ROMERA SANTIAGO, M.: *Hacia la implantación de la inteligencia artificial en nuestro sistema judicial*, Revista Aranzadi Doctrinal n° 3/2020 parte Estudios, BIB 2020\8846.

⁷ El *test de Turing* consiste en que un humano evalúa conversaciones en lenguaje natural entre un humano y una máquina, con el conocimiento previo de que uno de los participantes es una máquina. Si en 5 minutos de conversación, que equivale al 70% del tiempo en evaluación, el evaluador no es capaz de distinguir entre la máquina y el humano, aquélla habrá pasado la prueba.

⁸ ELIZA fue un dispositivo que incorporaba el procesamiento del lenguaje natural humano y cuyo principal objetivo era enseñar a los ordenadores a comunicarse con los seres humanos mediante su propio lenguaje y no mediante un lenguaje de programación.

ajedrez al entonces campeón del mundo Gari Kaspárov y surgieron los agentes de software inteligentes (que dieron pie a la posterior creación de sofisticados chatbots o a los asistentes virtuales actuales).

En el siglo XXI el crecimiento de la inteligencia artificial es imparable y se habla de la cuarta revolución humana⁹. En 2008 Google lanzó la primera aplicación con capacidad para reconocer la voz mediante el uso de la inteligencia artificial, en 2011 IBM presentó a WATSON, un ordenador que seguía la metodología DEEP BLUE y que consiguió ganar el concurso de preguntas y respuestas “Jeopardy!” superando a la mente humana, en 2012 las técnicas del machine learning estaban ya bastante optimizadas y las redes habían proporcionado a los investigadores enormes cantidades de datos, en 2014 un bot computacional llamado EUGENE GOOSTMAN superó el test de Turing y, en 2015, AlphaGo se convirtió en la primera máquina en ganar a un jugador profesional del juego oriental Go. A partir de aquí los logros se suceden sin freno; en 2013 se creó a ATLAS, un robot bípedo de rescate de la Boston Dynamics que era capaz de mantener el equilibrio y que posteriormente (2016) fue capaz de caminar por terrenos escarpados, de limpiar, de saltar (2017) y de hacer parkour (2018), en 2014 se diseñó EUGENE, la primera inteligencia artificial que se hizo pasar por una persona con éxito, en 2016 el MIT lanzó el primer taxi autónomo en Singapur, Uber trabajaba con coches robots en Pittsburg y San Francisco y DEEPMIND ganó al videojuego de estrategia Starcraft y AlphaGo al menor jugador del mundo de Go, en 2018 los residentes de Fénix (Arizona) podían descargarse una App para llamar a un taxi autónomo, AlphaZero se enseñaba a sí misma a jugar al ajedrez y en España se lanzó una inteligencia artificial llamada VERIPOL para detectar denuncias falsas¹⁰.

Este auge de la inteligencia artificial en los últimos años se debe fundamentalmente a la posibilidad de recogida, organización y almacenamiento de una gran cantidad de datos (macrodatos) y al aumento exponencial de la potencia de cálculo de los ordenadores y las capacidades de los algoritmos. Estas tres circunstancias -crecimiento de la capacidad informática, disponibilidad de datos y avances de los algoritmos- han convertido a la inteligencia artificial en una de las tecnologías más estratégicas del siglo XXI. Estamos ante la tecnología del porvenir, nutrida por datos. Su potencial supera con creces al que se ha visto hasta ahora; no obstante, sus repercusiones son todavía inciertas, pues se hallan en directa dependencia de diversos factores, entre otros la evolución política, normativa y económica y su aceptación

⁹ La expresión “cuarta revolución humana” fue acuñada por Schwab, quien defiende que han existido 3 revoluciones humanas comparables a la de la inteligencia artificial: la invención de la máquina de vapor (ss. XVIII y XIX), la invención de la electricidad (s. XX) y la invención de la computación (finales del s. XX).

¹⁰ En 2019 se registraron en ArXiv (archivo online para las publicaciones de artículos científicos en diversos campos, entre ellos el de las ciencias de la computación) un repositorio de estudios y casi 300 papers orientados a la inteligencia artificial.

social, de donde resulta la imposible previsión fiable de las consecuencias de su uso y normalización. Su presencia en nuestras vidas es incuestionable: ahí está cuando utilizamos un asistente personal para optimizar nuestra jornada laboral, cuando nos desplazamos en un vehículo de conducción automática, cuando hacemos uso de las sugerencias de nuestros dispositivos móviles para buscar restaurantes, tiendas u otros servicios, cuando nos servimos de aplicaciones para traducir un texto de un idioma a otro, cuando instalamos y usamos un termostato inteligente, etc.

La inteligencia artificial tiene potencial en multitud de áreas, completando la capacidad humana. En el ámbito asistencial, permite desarrollar funciones de prevención, de asistencia, de seguimiento, de estimulación y de compañía de personas mayores, discapacitadas y afectadas por enfermedades crónicas, así como mejorar su movilidad e integración, posibilitando, de esta suerte, que el personal médico dedique más tiempo al diagnóstico; en el sanitario, puede ayudar al personal en el diagnóstico y tratamiento de pacientes reduciendo el riesgo del error humano, permite la ejecución de cirugías de alta precisión y la realización de procedimientos repetitivos, mejora los resultados de la rehabilitación, proporciona apoyo logístico a los hospitales, posibilita centrar la atención del personal médico en la prevención (en lugar de en el tratamiento)¹¹ y ayuda al tratamiento de enfermedades crónicas y a la predicción de brotes de enfermedad; en el laboral, redundante en la creación de empleo¹² en ingeniería, informática y telecomunicaciones y en macrodatos (big data) y permite la realización de tareas repetitivas, extenuantes y peligrosas, mejorando así la seguridad en este sector; en el industrial, mejora la eficiencia de los sistemas de producción a través de su mantenimiento productivo; en el medioambiental, contribuye a la lucha contra el cambio climático al reducir el tamaño de la maquinaria y el uso de abonos, energía y agua y permite desarrollar la agricultura de precisión y la optimización de los circuitos de distribución; mejora los productos, procesos y modelos de negocio en todos los sectores económicos, mejora la seguridad de los productos y los hace menos propensos a los riesgos; mejora los servicios de interés público (por ejemplo, educación y transporte) al reducir sus costes y permite una mayor sostenibilidad de los recursos, proporcionando a las Fuerzas y Cuerpos de Seguridad las herramientas

¹¹ Por poner algún ejemplo a este respecto, en Dinamarca (Copenhage) desde el año 2016 se utiliza a CORTI (inteligencia artificial creada por una Startup holandesa con el mismo nombre) en los servicios de emergencias para diagnosticar paradas cardíacas y otras dolencias analizando la voz del sujeto que llama.

¹² Según el *Informe Artificial Intelligence Index Report 2019*, Singapur, Brasil, Australia, Canadá e India son los Países con mayor crecimiento en contrataciones para trabajos relacionados con la inteligencia artificial desde el 2015. En EEUU las ofertas de empleo relacionadas con la inteligencia artificial en 2019 ascendieron al 1,32% del total de las ofertas, mientras que en 2010 eran del 0,26%. La mayoría de estos puestos de trabajo están relacionados con el machine learning y, principalmente, con el sector de la fabricación y de servicios de alta tecnología. En la UE el número de especialistas en tecnologías de la información y la comunicación ha crecido un 5% anual desde el año 2011, lo que ha supuesto la creación de 1,8 millones de empleos, que se traduce en un 3,7% del empleo total.

adecuadas para mejorar la protección de los ciudadanos. Y éstos son sólo algunos ejemplos.

Todas estas ventajas de la inteligencia artificial han motivado un incremento de la venta de robots durante los últimos años. De acuerdo con un estudio de Robotics Industry Association (RIA), entre 2010 y 2014 las ventas aumentaron un 17% de media cada año, registrándose en 2014 el mayor incremento (un 29%). En 2017 se vendió un 31% más que en el año anterior y en el año siguiente, en 2018, se alcanzó un nuevo record de ventas, registrándose un incremento del 7% con respecto a 2017. En el sector de la robótica en alimentación, en 2018 se registró un incremento de ventas del 41% con respecto al 2017. Según el *Estudio Global Autonomous Delivery Robots Market*¹³ el negocio de los vehículos autónomos de reparto crecerá un 16% entre 2019 y 2025. No obstante, es más que obligado advertir que la actual situación de pandemia afectará a estos porcentajes, siendo previsible una disminución (se habla de hasta un 30%) de la venta de robots como consecuencia de la desaceleración económica que se está produciendo a nivel global. Sin embargo, no es menos cierto que la pandemia ha acelerado el impulso de una automatización que, si antes ya tenía sentido, en el contexto descrito resulta indispensable. Los robots están siendo utilizados por algunos Países para reducir el contacto entre humanos y mantener la distancia social recomendada; por mencionar algunos supuestos concretos, en Corea del Sur CABO sirve bebidas en Coffe Bark¹⁴, los Países Bajos también utilizan robots meseros, Ruan-da cuenta con profesionales de la salud robóticos que ayudan a los médicos humanos que combaten el COVID en primera línea y que desarrollan aproximadamente el 50% del trabajo técnico (toman la temperatura y los signos vitales y entregan mensajes de video o comentarios entre médicos y pacientes, entre otras cosas) y en Singapur el canino robótico SPOT transita por las calles y espacios públicos para comprobar el cumplimiento de la distancia social.

Pero no nos llevemos a engaño; no todo son ventajas. La inteligencia artificial también tiene ciertos e importantes inconvenientes, entre los que pueden destacarse, sin ánimo exhaustivo, la eliminación de puestos de trabajo a cuenta de los robots inteligentes¹⁵, la posible discriminación de género, por motivos raciales o de origen étnico, religión o credo, discapacidad o edad, la intromisión en la intimidad¹⁶, su uso con

¹³ Estudio elaborado por varias empresas de robótica, entre ellas pueden citarse Carbon Robotics, Anybot Autonomous Solutions, Starship Technology, Aethon y 3D Robotics.

¹⁴ Se estima que en los próximos meses abrirán sus puertas con esta tecnología 30 nuevos Cafés.

¹⁵ De acuerdo con un Estudio divulgado por el más reciente Foro Económico de Davos, más de 7 millones de empleos se verán afectados. Los puestos de trabajo vinculados a la nueva actividad serán muchos menos y, por lo tanto, insuficientes para evitar una pérdida neta. Vide MARTÍNEZ, D.: ¿Un mundo sin empleo humano?, Actualidad Económica, Madrid, mayo 2017, <https://search.proquest.com>.

¹⁶ Por ejemplo, los drones que incorporan cámaras y que graban su entorno pueden vulnerar los derechos a la intimidad y a la imagen. También los dispositivos domésticos conectados a internet pue-

fines fraudulentos¹⁷ y la concentración de la riqueza y del poder en manos de una minoría. A estas posibles desventajas debe sumarse el temor socialmente generalizado a una posible rebelión de los robots, que se conoce como “síndrome de Frankenstein”, por ser precisamente la autora de esta novela (Frankenstein o El Modelo Prometeo, publicada el 1 de marzo de 1818), Mary Shelley, una de las primeras personas en abordar la citada reflexión. Esta preocupación encuentra su reflejo en el sector del cine, en películas como “Yo, robot” (adaptación de una de las novelas de Isaac Asimov), “I am mother” (reelaboración del mito de Colossus de Dennis Feltham Jones) y “Ex Machina” y en series como “Westworld”. El propio Parlamento Europeo se hace eco de este miedo en su Resolución de 16 de febrero de 2017, en la que hace alusión a las *Leyes de Asimov* (Leyes de la Robótica, Runaround, 1942)¹⁸ y dispone que las mismas se dirigen a diseñadores, fabricantes y operadores de robots. Ello justifica la conexión de la robótica con la ética; precisamente por este temor y ante la previsión de posibles daños, la Resolución citada del Parlamento Europeo incluye varias recomendaciones éticas a las que se acompañan un “Código de conducta ética para los ingenieros en robótica” y un “Código deontológico para los Comités de ética de la investigación”.

En efecto, la inteligencia artificial puede producir daños (materiales e inmateriales) que pueden estar vinculados a una gran variedad de riesgos, siendo destacables los que afectan a la aplicación de las normas protectoras de los derechos fundamentales y la seguridad y las cuestiones relativas a la responsabilidad civil. Puede conculcar los derechos (entre los que pueden citarse la dignidad, la igualdad, la justicia y la equidad, la no discriminación, la vida privada y la protección de datos) y valores fundamentales (entre ellos, la transparencia, la autonomía, la no estigmatización y la responsabilidad individual y social) en que se asienta la Unión Europea como consecuencia de defectos en su diseño general, en especial en lo concerniente a la supervisión humana, o del uso de datos que puedan ser sesgados sin una corrección previa (como ocurre, por ejemplo, cuando se entrena un sistema utilizando única o principalmente datos relativos al hombre y ello se traduce en resultados peores en relación a las mujeres)¹⁹. Además, las características propias y específicas de las tecnologías digitales pueden dificultar la determinación del sujeto responsable del daño y, en con-

den transmitir datos personales sin el permiso del usuario, lo cual, además del derecho a la intimidad, vulneraría el derecho fundamental a la protección de los datos de carácter personal.

¹⁷ Puede, por ejemplo, permitir a empresas, autoridades y otros organismos observar el comportamiento de sus empleados y ciudadanos, respectivamente, para rastrear y desanonimizar datos, contraviniendo así las normas en materia de protección de datos.

¹⁸ 1. Un robot no hará daño a un ser humano ni permitirá que, por inacción, éste sufra daño; 2. Un robot obedecerá las órdenes que reciba de un ser humano a no ser que las órdenes entren en conflicto con la primera ley; 3. Un robot protegerá su propia existencia en la medida en que dicha protección no entre en conflicto con las leyes primera y segunda; 0. Un robot no hará daño a la humanidad ni permitirá que, por inacción, ésta sufra daño.

¹⁹ Libro Blanco sobre la Inteligencia Artificial -un enfoque europeo orientado a la excelencia y la confianza, Bruselas, 19 de febrero de 2020 (COM(2020)65 final).

secuencia, reducir las posibilidades de éxito de una reclamación de responsabilidad civil; dichas características son las siguientes²⁰:

1. Complejidad: Las tecnologías digitales se caracterizan por una combinación de hardware y software. El hardware se halla integrado por una pluralidad de partes o de componentes digitales, siendo en ocasiones complicado determinar cuál de esos componentes (piezas o algoritmos) ha sido el causante del daño, lo cual a su vez dificulta la aplicación de las normas sobre responsabilidad civil.
2. Opacidad: El código de funcionamiento de los dispositivos digitales se integra de algoritmos, que a veces son complicados de entender (incluso para los propios expertos), sobre todo cuando incorporan las características del autoaprendizaje (machine learning). Ello puede dificultar la determinación del sujeto que controlaba el riesgo, o del código, entrada o datos que han dado lugar al funcionamiento lesivo, lo cual, a su vez, dificultaría la identificación de la relación (relación causal) entre el daño y la conducta causante del mismo, con la consecuencia de que las víctimas podrían verse privadas de una justa indemnización.
3. Apertura: Los sistemas que sirven de base a las tecnologías digitales están normalmente abiertos a actualizaciones y a mejoras posteriores a su puesta en circulación, incluso en ocasiones, interactúan con otros sistemas o fuentes de datos para funcionar correctamente y ello puede obstaculizar la correcta aplicación de la normativa sobre responsabilidad civil por productos defectuosos.
4. Autonomía: El Parlamento Europeo²¹ define “sistema de inteligencia artificial autónomo” como «todo sistema de inteligencia artificial que funciona interpretando determinados datos de entrada y utilizando un conjunto de instrucciones predeterminadas, sin limitarse a ellas, a pesar de que el comportamiento del sistema esté limitado y orientado a cumplir el objetivo que se le haya asignado y otras decisiones pertinentes de diseño tomadas por su desarrollador». Las tecnologías digitales están diseñadas para funcionar de forma autónoma, prácticamente sin control o supervisión humana, lo que

²⁰ ATAZ LÓPEZ, J.: *Daños causados por las cosas: una nueva visión a raíz de la robótica y de la Inteligencia artificial*, Working Papers, Universitat de Barcelona, Working Paper 4/2020, p. 18, texto que es una reproducción de un trabajo realizado en el marco del Proyecto de Investigación nº PGC2018-098206 B del Ministerio de Ciencia, Innovación y Universidades, titulado *El derecho de contratos en el entorno digital* y que ha sido previamente publicado como capítulo del Libro *Derecho de daños*, dir. por HERRADOR GUARDIA, Lefebvre 2020, pp. 317-375.

²¹ *Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial*, incluido en el *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL)), de 5 de octubre de 2020 (Vide art. 3, apartado b).

añadido al autoaprendizaje, puede dar lugar a una disociación entre la conducta humana y la acción del dispositivo que dificulta la determinación del responsable del daño.

5. Imprevisibilidad: La acción del dispositivo es difícilmente previsible, lo cual complica la imputación de responsabilidad basada en la culpa a quien se beneficia de él.
 6. Vinculación a datos externos: Puede ocurrir que el dispositivo dotado de inteligencia artificial produzca un daño como consecuencia de datos defectuosos o corrompidos que haya recogido con posterioridad a su diseño y fabricación, en cuyo caso será muy difícil reclamar responsabilidad al diseñador, al programador, al fabricante o a la persona que se sirva de dicho dispositivo.
 7. Vulnerabilidad: Los dispositivos dotados de inteligencia artificial son vulnerables a los ciberataques como consecuencia de su apertura a actualizaciones y mejoras, de su interconectividad y del consumo de datos externos, daños de los que difícilmente puede responsabilizarse a los fabricantes, diseñadores, programadores o usuarios.
3. LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL: ACTUALIZACIÓN DEL MARCO JURÍDICO EUROPEO Y DE LOS MARCOS JURÍDICOS NACIONALES VERSUS CREACIÓN DE INSTRUMENTOS JURÍDICOS NUEVOS Y ESPECÍFICOS

3.1. El eterno debate

La citada potencial afectación de la inteligencia artificial en todos los estratos de la sociedad, aconseja una ponderación legislativa de sus consecuencias jurídicas. Su uso puede comportar riesgos que deben ser previstos y mitigados; en particular, es preciso aclarar la atribución de la correspondiente responsabilidad civil por dichos daños, concretar su fundamento y fijar los criterios para la determinación de la correspondiente indemnización. Es menester, en otras palabras, establecer un marco jurídico²² a escala de la Unión Europea que refleje sus valores y derechos fundamentales sin obstaculizar

²² Existe ya legislación sobre robots en Corea del Sur (Korean Law on the Development and Distribution of Intelligent Robots 2005 y Legal Regulation of Autonomous Systems in South Korea 2012) y en Japón (Guidelines to Secure the Safe Performance of Next Generation Robots y New Robot Strategy -Japan's Robot Strategy- Vision, Strategy, Action Plan y Headquarters for Japan's Economic Revitalization 2015). Estas normas responden a una triple necesidad común: la regulación de la responsabilidad civil por daños causado por robots, las cuestiones éticas derivadas de la relación robot/humano y el posible reconocimiento de la personalidad jurídica de los robots.

la investigación y el desarrollo, en síntesis, sin poner trabas a la innovación. Se trata de evitar el denominado *chilling effect* (la rigidez de las normas obstaculiza la innovación de los productos y servicios). Las iniciativas nacionales²³ incidirían en la temida fragmentación del mercado único, poniendo en peligro la seguridad jurídica y reduciendo la confianza de los ciudadanos en la interacción con estas tecnologías. El enfoque debe ser Europeo, dadas las implicaciones transfronterizas que pueden surgir con la creación y la comercialización de sistemas dotados de inteligencia artificial en los diversos Estados Miembros. Es fundamental una legislación uniforme; tal y como argumenta el propio Parlamento Europeo²⁴, si bien son preferibles reglamentaciones sectoriales específicas para la amplia gama de posibles aplicaciones, parece necesario contar con un marco jurídico horizontal y armonizado basado en principios comunes con el fin de garantizar la seguridad jurídica, establecer una igualdad de normas en toda la Unión y proteger eficazmente los valores y derechos de los ciudadanos europeos. Ciudadanos y empresas precisan de un marco jurídico claro y estable que les garantice su interacción con estas tecnologías digitales y que sus derechos y libertades fundamentales van a ser respetados. Mas el reiterado marco jurídico debe ser extremadamente cauteloso y ponderar todos los intereses en juego.

Pues bien, el interrogante que se ha venido planteando a este respecto durante años es el siguiente: ¿es suficiente con actualizar y completar las regulaciones nacionales y el marco jurídico europeo o es preciso adoptar nuevos y específicos instrumentos jurídicos?

En el año 2012 la Comisión Europea financió el denominado *Proyecto Robolaw*, que concluyó en mayo de 2014 y cuyo objetivo era la elaboración de un Informe detallado con todas las cuestiones éticas y legales que plantean los robots y con orientaciones y principios que pudieran guiar a los legisladores nacionales y europeos en la reglamentación de la materia (*Guidelines on Regulating Robotics*, octubre 2014). Dicho Informe se centró en el tema de la responsabilidad, planteando ideas como la concesión de personalidad electrónica a los robots, la limitación de la responsabilidad de los fabricantes otorgando cierta inmunidad selectiva en el caso de plataformas abiertas y la fijación de un límite en la cantidad de los daños a compensar. En dicho

²³ En Alemania, el Comité de la Agenda Digital celebró el 22 de junio de 2016 una sesión sobre *los efectos de la robótica en la economía, el trabajo y la sociedad*. También en el año 2016, en el mes de marzo, el Parlamento Británico emitió una Consulta pública en la que se planteó, entre otros temas, las implicaciones de la robótica y la inteligencia artificial en el mercado de trabajo, la forma de explotación de sus oportunidades (sociales y económicas) para procurar beneficios al País, los problemas sociales, legales y éticos vinculados a su evolución y la forma en que deben ser tratados y las medidas a adoptar para ayudar en la financiación, la investigación y la innovación en estas materias. Vide SANCHEZ DEL CAMPO REDONET, A.: *Europa quiere regular a los robots*, Diario La Ley, n1 4, sección Ciberderecho, 28 de febrero de 2017, Ed. Wolters Kluwer, La Ley 2253/2017.

²⁴ *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL))*, de 5 de octubre de 2020.

Informe se cuestionó si era necesaria una Ley Robótica y si era precisamente ese el momento adecuado para regular una materia tan novedosa cuyos efectos eran (y son todavía) más que imprevisibles.

A principios de 2015 la Comisión de Asuntos Legales del Parlamento Europeo (Comisión JURI) creó el Grupo de Trabajo (GT) sobre Cuestiones Jurídicas relacionadas con el Desarrollo de la Robótica, para la reflexión sobre cuestiones jurídicas y, especialmente, para preparar el terreno para la redacción de normas civiles relativas a la robótica y a la inteligencia artificial. Su misión era precisamente la de estimular la reflexión al respecto por parte de los Estados Miembros, facilitándoles información específica y diversos puntos de vista expertos para el análisis de los desafíos y de las perspectivas en juego. El *Proyecto de Informe sobre Normas de Derecho Civil sobre Robótica*²⁵, que describió el marco principal y la visión del Parlamento Europeo sobre la robótica y la inteligencia artificial, se hizo público en junio de 2016, aprobándose el 27 de enero de 2017 el texto definitivo. El Informe propuso la creación de una personalidad jurídica específica para los robots autónomos más complejos que toman decisiones inteligentes interactuando con terceros de forma independiente, de suerte que pudieran ser considerados como personas electrónicas responsables de reparar los daños que pudieran causar. Consideró que cuanto mayor fuera la capacidad de aprendizaje o la autonomía del robot, mayores serían las posibilidades de poder hacer efectiva sobre el mismo una reparación; identificada la parte (o las partes) responsable(s), lo justo es que la responsabilidad del robot sea proporcional a las instrucciones recibidas y a su autonomía, de manera que cuanto mayor sea su capacidad de aprendizaje autónomo mayor será su responsabilidad y menor la del agente humano instructor y viceversa. En este orden de cosas, el Informe puso de manifiesto una realidad que ya había sido objeto de debate doctrinal y es que en el actual marco normativo los robots que toman decisiones autónomas no pueden considerarse como responsables de sus actos y omisiones que causen daño a terceros, ya que no permite determinar la parte que debe hacerse cargo de la reparación del daño. Igualmente destacó la inaplicabilidad de la normativa en materia de Propiedad Intelectual, instando a que se aclararan las cuestiones relativas a la creación intelectual propia de los robots autónomos avanzados, así como de las normas relativas a la protección de la intimidad desde el diseño y por defecto, al consentimiento informado y al cifrado y al uso de datos personales.

En la Resolución de 16 de febrero de 2017 (*Normas de Derecho Civil sobre Robótica*)²⁶ el Parlamento Europeo pidió a la Comisión, sobre la base del artículo 225 del Tratado Fundacional de la Unión Europea (TFUE) la redacción de una propuesta

²⁵ *Proyecto de Informe con recomendaciones a la Comisión de normas de Derecho Civil sobre Robótica* (2015/2013(INL), Ponente Mady Delvaux (S&D, Luxemburgo), 31 de mayo de 2016, PE582.443 01-00.

²⁶ Resolución del Parlamento Europeo de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre Robótica (2015/2013 (INA) P8_TA(2017)0051).

de Directiva, sobre la base del artículo 114 del mismo texto legal, relativa a las normas de legislación civil en materia de robótica tomando como base las recomendaciones detalladas en su Anexo y que pueden sintetizarse del siguiente modo:

1. Elaboración de una definición común de robots autónomos «inteligentes» que comprenda las siguientes características: interconectividad, capacidad de autoaprendizaje, forma del soporte físico del robot y capacidad para adaptar su comportamiento y acciones al entorno. El tema conceptual no es baladí, ya que del mismo va a depender la cuestión de la responsabilidad civil por los daños causados por el uso de estas tecnologías digitales.
2. Introducción de un sistema de registro de robots avanzados y creación de una Agencia para la robótica y la inteligencia artificial.
3. En concreto, en sede de responsabilidad civil, se plantean las siguientes recomendaciones:
 - a. La solución que se adopte en este ámbito en ningún caso debería limitar el tipo o el alcance de los daños y perjuicios compensables, ni la naturaleza de esta compensación, en base exclusivamente a que aquellos no han sido causados por un agente humano.
 - b. Debería definirse si el enfoque a aplicar es el de la responsabilidad objetiva o el de gestión de riesgos.

En este punto se modifica la postura inicial del Parlamento Europeo, que apostaba por la aplicación del principio de responsabilidad objetiva.
 - c. Podría graduarse la responsabilidad en función de la capacidad de aprendizaje del robot, debiendo ser la responsabilidad de las partes implicadas proporcional al nivel de instrucciones impartidas al robot y a su autonomía, de forma que, cuanto mayor sea la capacidad de aprender o la autonomía del robot menor será la responsabilidad de las partes y cuanto más se haya prolongado la instrucción del robot mayor será el grado de responsabilidad del instructor.
 - d. Sería aconsejable el establecimiento de un régimen de seguro obligatorio, que podría basarse en la obligación del productor de suscribir un seguro para los robots fabricados por él y que debería completarse con un fondo que garantice la compensación de los daños y perjuicios en los supuestos en que no exista una cobertura de seguro.
4. Teniendo en cuenta que la autonomía de los robots para tomar decisiones aumenta de forma paralela al desarrollo de la inteligencia artificial, plantea la cuestión sobre la naturaleza legal de los mismos y sobre si encajan o no en

alguna de las categorías existentes (personas físicas, personas jurídicas, animales y objetos), propone crear a largo plazo una personalidad jurídica específica, de manera que al menos los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de los daños que puedan causar y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas e inteligentes o interactúen con terceros de forma independiente.

En rigor el Parlamento Europeo no se pronuncia a favor de la alternativa de atribuir una personalidad electrónica a los robots; simplemente requiere a la Comisión para que valore las implicaciones de diversas posibilidades, entre las que se encontraba esta.

5. Debería garantizarse la interoperabilidad de los robots conectados a la red autónoma que interactúan entre sí. Sería aconsejable facilitar la accesibilidad al código fuente, a los datos de entrada y a los detalles de construcción cuando ello fuera necesario para investigar los daños causados por los mismos y para velar por su funcionamiento, disponibilidad, fiabilidad, seguridad y protección continuados. Se enfatiza así el principio de transparencia (siempre debe ser posible justificar cualquier decisión que se haya adoptado con la ayuda de la inteligencia artificial y que pueda tener un impacto significativo sobre la vida de una o varias personas) y se considera que siempre debe ser posible reducir los cálculos del sistema de inteligencia artificial a una forma comprensible para los humanos; en esta línea se recomienda que los robots avanzados estén dotados de una «caja negra» que registre todas las operaciones efectuadas por aquéllos, incluidos, en su caso, los pasos lógicos que han conducido a la formulación de sus decisiones.

Poco más de un año después, el 25 de abril de 2018, la Comisión Europea expuso una iniciativa europea sobre la inteligencia artificial en su *Comunicación Inteligencia artificial para Europa (Artificial Intelligence for Europe)*²⁷, en la que propuso un enfoque que coloca a las personas en el centro del desarrollo de la inteligencia artificial (inteligencia artificial centrada en el ser humano) y entre cuyos fines figuraba el de garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión y en consonancia con la Carta de los Derechos Fundamentales de la Unión Europea²⁸. La Comunicación incluyó una próxima directriz sobre la interpretación de las actuales normas en materia de seguridad y de responsabilidad por productos defectuosos y un análisis pormenorizado de los retos emergentes. Reconoció que se estaba evaluando si, teniendo en cuenta los nuevos desafíos que plantea

²⁷ COM(2018)237 final, SWD(2018)137 final.

²⁸ Los otros dos pilares de la Estrategia son: el aumento de las inversiones, públicas y privadas y la preparación de la sociedad para los cambios socioeconómicos.

la inteligencia artificial, los marcos en materia de seguridad y los marcos nacionales y de la Unión Europea en materia de responsabilidad civil son adecuados para el fin previsto o existen lagunas que deben colmarse y que se habían llevado a cabo las evaluaciones, a este respecto, de la Directiva sobre la responsabilidad por los daños causados por productos defectuosos y de la Directiva sobre máquinas, así como de los marcos en materia de responsabilidad a la luz de la inteligencia artificial y las tecnologías emergentes. A estos efectos, la Comisión se comprometió a publicar, a más tardar a mediados de 2019, un documento de orientación para la interpretación de la Directiva sobre responsabilidad por los daños causados por productos defectuosos con el objetivo de garantizar la claridad jurídica para los consumidores y para los productores en caso de productos defectuosos y un Informe acerca de los marcos en materia de responsabilidad y de seguridad en relación con la inteligencia artificial, el internet de las cosas y la robótica, en el que se analizarían las repercusiones de carácter general y las posibles lagunas y se expondrían las correspondientes directrices. La citada Comunicación concluyó con la afirmación de que la Unión Europea dispone de un marco jurídico completo que protege a los consumidores al tiempo que favorece la innovación.

La Comisión propuso elaborar un Plan Coordinado con los Estados Miembros para finales del 2018 entre cuyos fines figuraba el de abordar las cuestiones de carácter ético y jurídico. Este *Plan Coordinado sobre la Inteligencia artificial* figura como Anexo a la Comunicación de 7 de diciembre de 2018²⁹, que detalló las acciones que se iniciarían en el 2019-2020 y preparaba el terreno para las actividades en los años siguientes³⁰. El Plan Coordinado ofreció un marco estratégico para las Estrategias Nacionales de Inteligencia artificial, alentando a los Estados Miembros a desarrollar su propia Estrategia para mediados de 2019 en base al trabajo realizado a nivel Europeo³¹. Reitera en

²⁹ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Plan Coordinado sobre la Inteligencia artificial, Bruselas, 4 de diciembre de 2018, COM(2018)795 final.

³⁰ Se detalla que el Plan Coordinado será revisado y actualizado anualmente.

³¹ En España, en concreto, Pedro Sánchez ha presentado recientemente, el 2 de diciembre de 2020, la Estrategia Nacional de Inteligencia artificial (ENIA) (<https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf>) con el objetivo de generar un entorno de confianza respecto al desarrollo de una inteligencia artificial inclusiva, sostenible y que ponga a la ciudadanía en el centro. Los 6 ejes estratégicos de la ENIA son:

— Impulso de la investigación científica, el desarrollo tecnológico y la innovación en inteligencia artificial.

— El fomento de las capacidades digitales, el desarrollo del talento nacional y la atracción del internacional.

— El desarrollo de plataformas de datos e infraestructuras tecnológicas que den soporte a la inteligencia artificial.

— Integrar la inteligencia artificial en las cadenas de valor para transformar el tejido económico.

— Impulsar el uso de la inteligencia artificial en la Administración Pública y en las misiones estratégicas nacionales.

este documento que se estaba evaluando si los marcos de seguridad y de responsabilidad nacionales y de la Unión Europea son aptos para el propósito a la luz de los nuevos desafíos que plantean las tecnologías digitales o si deben abordarse las deficiencias y se compromete a publicar, a mediados de 2019, un Informe sobre las posibles brechas y orientaciones para estos marcos con respecto a la inteligencia artificial.

Cumpliendo con estos compromisos, la Comisión presentó, a mediados del 2020, el *Libro Blanco sobre la Inteligencia Artificial - Un enfoque europeo orientado a la excelencia y la confianza*³², en el que se ofrecen alternativas políticas para facilitar un desarrollo de la inteligencia artificial seguro y fiable en Europa que respete plenamente los valores y los derechos de los ciudadanos europeos y cuyos pilares fundamentales son los dos siguientes: 1. El marco político por el que se establecen medidas para armonizar los esfuerzos a escala regional, nacional y europea; 2. Los elementos clave de un futuro marco normativo que genere un «ecosistema de confianza» exclusivo. En esta sede la Comisión respalda firmemente un enfoque antropocéntrico que se base en la *Comunicación Generar confianza en la inteligencia artificial centrada en el ser humano*³³. Considera conveniente mejorar el marco normativo europeo para abordar los siguientes riesgos y situaciones:

1. Dada la dificultad que las características de la inteligencia artificial (como por ejemplo la opacidad) plantean en la detección y demostración de posibles incumplimientos de la legislación vigente (especialmente de las normas protectoras de los derechos fundamentales, sobre responsabilidad e indemnización), es necesario clarificar dicho marco en algunos sectores, como sucede con el concerniente a la responsabilidad civil.
2. La legislación general de la Unión Europea en materia de seguridad es aplicable a los productos, pero no a los servicios, entre ellos a los servicios basados en inteligencia artificial (por ejemplo, servicios financieros o de transporte). También se duda si un programa informático autónomo se rige por esta legislación de seguridad de productos (salvo aquellos sectores, como el sanitario, que cuentan con normas explícitas).
3. La legislación vigente no aborda los riesgos que pueden derivarse de las actualizaciones informáticas o del aprendizaje automático; al contrario, se centra en los riesgos de seguridad al tiempo de la comercialización.

— El establecimiento de un marco ético y normativo que garantice la protección de los derechos individuales y colectivos a efectos de garantizar la inclusión y el bienestar social. A este respecto se pondrá en marcha un observatorio para evaluar el impacto social de los algoritmos, se desarrollará un sello nacional de calidad en inteligencia artificial y se elaborará una Carta de Derechos Digitales (<https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2020/021220-sanchezenia.aspx>).

³² Bruselas, 19 de febrero de 2020, COM(2020)65 final.

³³ COM(2019)168.

4. La legislación vigente puede ser poco clara en orden a la imputación de responsabilidades entre los distintos agentes económicos de la cadena de suministro. Imputa la responsabilidad al productor del producto comercializado (incluidos sus componentes, como los sistemas de inteligencia artificial), pero su aplicación puede ser dudosa cuando el producto se ha comercializado por alguien que no es el productor. Además, la legislación europea regula sólo la responsabilidad de los productores y deja al arbitrio de las normas nacionales la de los demás participantes de la cadena de suministro.
5. Deben introducirse cambios en el concepto de seguridad, teniendo en cuenta que los riesgos derivados del uso de las tecnologías digitales pueden estar vinculados a ciberamenazas, a la seguridad personal, a la pérdida de conectividad...y existir tanto al tiempo de comercializarse el producto o surgir después como consecuencia de actualizaciones del programa informático y del aprendizaje automático.

Por todo lo anterior la Comisión llega a la conclusión de que, además de posibles adaptaciones de la legislación vigente, puede que sea precisa una nueva legislación específica sobre la inteligencia artificial, a fin de adaptar el marco normativo europeo a la evolución tecnológica actual y futura. En efecto, la Unión Europea cuenta con un marco jurídico para garantizar la protección de los consumidores, la protección de los datos personales y la privacidad y con normas específicas en sectores concretos, como la sanidad y el transporte, que serán aplicables con relación a la inteligencia artificial, si bien son precisas ciertas actualizaciones que reflejen la transformación digital y el uso de la inteligencia artificial. No obstante, puede que sea necesaria la elaboración de una nueva legislación específica que siga un enfoque basado en el riesgo, con criterios claros de diferenciación entre las distintas aplicaciones de inteligencia artificial, en especial para determinar si entrañan o no un riesgo elevado³⁴; considera que una inteligencia artificial debe considerarse de riesgo elevado cuando concurren los dos criterios siguientes: a) que se emplee en un sector en el que, por las características o actividades que se llevan a cabo normalmente, es previsible que existan riesgos significativos (por ejemplo, sanidad y transporte) y b) que en el sector en cuestión se use la inteligencia artificial además de manera que puedan surgir riesgos significativos.

A este Libro Blanco se adjuntó el *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*³⁵, cuyo objetivo es determinar y analizar las repercusiones de carácter ge-

³⁴ Debe entenderse de riesgo elevado la inteligencia artificial en función lo que esté en juego y considerando si tanto el sector como el uso previsto suponen riesgos significativos, en especial desde la perspectiva de la protección de la seguridad, los derechos de los consumidores y los derechos fundamentales.

³⁵ Bruselas, 19 de febrero de 2019 COM(2020)64 final.

neral y los posibles resquicios jurídicos de los marcos en materia de responsabilidad civil y seguridad de la inteligencia artificial, el internet de las cosas y la robótica, pero que, tal y como advierte, no pretende ofrecer una perspectiva exhaustiva de la normativa vigente en estos ámbitos o materias, sino que se centra en las cuestiones clave. Analiza si el actual marco jurídico en estas materias sigue siendo adecuado para proteger a los usuarios y en qué medida; en concreto, reflexiona sobre las siguientes cuestiones:

1. Si la normativa sobre seguridad de los productos, principalmente la Directiva relativa a la seguridad general de los productos (Directiva 2001/95/CE), es suficiente para garantizar que las tecnologías emergentes y, en particular, la inteligencia artificial, integran funcionalidades de seguridad y de seguridad desde el diseño. A este respecto considera que gran parte de esta normativa es anterior a la aparición de esta tecnología, de suerte que no incorpora disposiciones que traten específicamente los riesgos asociados a la misma, pero que no obstante dicha normativa es neutra y, por lo tanto, puede aplicarse a los productos que incorporan tales tecnologías digitales. Otros actos normativos posteriores sí incorporan, en cambio, aspectos ligados a las mismas (piénsese en la automatización de las decisiones, en la consideración de los programas informáticos como productos independientes y en la conectividad), como ocurre por ejemplo en los sectores de los productos sanitarios y de los automóviles. Describe en este contexto una serie de dificultades que se aprecian en relación con las características propias de la inteligencia artificial:
 - a) La conectividad pone en jaque el concepto tradicional de seguridad. La normativa de la Unión en materia de seguridad de los productos no establece requisitos esenciales obligatorios específicos frente a las ciberamenazas que afectan a la seguridad de los usuarios. Sí existen, en cambio, disposiciones en materia de seguridad en el Reglamento (UE) 2017/745 sobre los productos sanitarios, en la Directiva 2014/32/UE sobre la comercialización de instrumentos de medida, en la Directiva 2014/53/UE sobre equipos radioeléctricos y en el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las utilidades técnicas independientes destinados a dichos vehículos. El Reglamento (UE) 2019/881 sobre la ciberseguridad establece marcos voluntarios de certificación de la ciberseguridad para productos, servicios y procesos de tecnologías de la información y la comunicación y la normativa de la Unión pertinente en materia de seguridad de los productos establece requisitos obligatorios. De otro lado, la pérdi-

da de conexión también puede entrañar riesgos relacionados con la seguridad.

A este respecto considera la Comisión que el concepto de seguridad de la normativa europea vigente abarca la protección contra todo tipo de riesgos derivados de los productos, no sólo los mecánicos, químicos y eléctricos, sino también los cibernéticos y los relacionados con la pérdida de conexión. No obstante, se podría contemplar adoptar disposiciones explícitas en relación con el ámbito de aplicación de los actos normativos de la Unión con el fin de ofrecer una mayor protección a los usuarios y una mayor seguridad jurídica.

- b) La autonomía puede dar lugar a resultados no deseados y perjudiciales producidos por los sistemas de inteligencia artificial no determinables por adelantado. El marco normativo ya establece obligaciones para que los productores, en la evaluación del riesgo, tengan en cuenta el uso de los productos a lo largo de su vida útil, a lo que se añade que, cuando tengan conocimiento de que un producto presenta riesgos en materia de seguridad a lo largo de su ciclo de vida, deberán informar automáticamente a la autoridad competente y tomar medidas de prevención de riesgos para los usuarios. También dispone la obligación de los fabricantes de ofrecer instrucciones e información de seguridad. Pero nada dice para el caso de que el uso inicialmente previsto por el fabricante se vea modificado hasta el punto de que pueda repercutir en su seguridad. Ante tal circunstancia la Comisión considera que, además de la evaluación del riesgo efectuada antes de la comercialización del producto, se podría establecer un nuevo procedimiento de evaluación del riesgo para dichos supuestos y, con carácter adicional, añadir requisitos reforzados para los fabricantes sobre las instrucciones y advertencias para los usuarios.

También deberían contemplarse requisitos específicos de supervisión humana que sirvan de salvaguarda desde el diseño y durante todo el ciclo de vida de los productos y sistemas de inteligencia artificial, requisitos que no están tampoco tratados por la normativa vigente.

El comportamiento de las aplicaciones de inteligencia artificial podría generar riesgos para la salud mental de los usuarios. Dado que en la actualidad la seguridad se refiere normalmente a la percepción del usuario de una amenaza de daño físico que puede derivarse de la tecnología digital y dado que se configura como producto seguro el que no presenta riesgo o solo el riesgo mínimo para la seguridad y la salud de las personas (concepto este último que incluye tanto el bienestar fí-

sico como el mental), la Comisión entiende que podría contemplarse incluir en la normativa obligaciones explícitas de los productores para que valoren el citado daño moral.

- c) La dependencia de los datos también puede generar riesgos para la seguridad, derivados de datos erróneos, tema éste tampoco tratado en la normativa vigente. Por ello la Comisión plantea la inclusión de requisitos específicos en la fase de diseño relacionados con tal riesgo y de mecanismos que garanticen la calidad de los datos.
- d) La legislación europea tampoco trata explícitamente el tema del aumento de riesgos derivados de la opacidad de los sistemas basados en algoritmos. Por ello contempla la posibilidad de introducir requisitos de transparencia de los algoritmos, de solidez, de rendición de cuentas y, cuando proceda, supervisión humana y resultados imparciales, lo cual reviste importancia para el mecanismo de control *a posteriori*. Se propone, como forma de afrontar esta cuestión, la imposición de obligaciones a los desarrolladores de los algoritmos de revelación de los parámetros de diseño y los metadatos de los conjuntos de datos si se producen accidentes.
- e) La complejidad de los productos y sistemas de inteligencia artificial también puede generar riesgos para la seguridad. La normativa vigente ya tiene en cuenta esta complejidad para hacer frente a los riesgos (Reglamento (CE) 765/2008 y Decisión 768/2008/CE y la normativa sectorial armonizada sobre seguridad de los productos, por ejemplo la Directiva 2006/42/CE sobre máquinas). En concreto, cuando el productor realice la evaluación del riesgo del producto deberá tener en consideración el uso previsto, el uso previsible y el mal uso previsible y por ello, si prevé que su dispositivo estará interconectado o interactuará con otros dispositivos, deberá considerar este aspecto en la evaluación del riesgo.

También se trata el tema de la complejidad en la normativa sectorial de seguridad, como por ejemplo el Reglamento sobre los productos sanitarios y la Directiva relativa a la seguridad general de los productos y a nivel del sistema en la normativa en materia de transporte.

Otra cuestión contemplada es la de los riesgos derivados para la seguridad de los programas informáticos integrados en un producto en el momento de su comercialización y de actualizaciones futuras previstas por el fabricante, respecto de la cual se afirma que, aun cuando la normativa de la Unión tiene en cuenta estos riesgos, pueden ser precisos requisitos específicos y/o explícitos para los programas infor-

máticos autónomos (por ejemplo, una aplicación que se descargue), debiendo tenerse en cuenta especialmente aquellos que garantizan las funciones de seguridad de los productos y sistemas de inteligencia artificial. Pueden ser también necesarias obligaciones adicionales para los fabricantes a fin de garantizar que ofrezcan funcionalidades para evitar la introducción de programas informáticos que afecten a la seguridad durante la vida útil de los productos de inteligencia artificial.

- f) La normativa tiene en cuenta la complejidad de las cadenas de valor e impone obligaciones a una serie de agentes económicos en consonancia con el principio de responsabilidad compartida. Los productores son responsables de la seguridad del producto final, incluidas las partes integradas en el mismo (por ejemplo, los programas informáticos de un ordenador). Y si bien esta responsabilidad ha resultado adecuada para las cadenas de valor complejas actuales, contar con disposiciones explícitas que pidan específicamente la cooperación entre los agentes económicos de la cadena de suministro y los usuarios puede aportar seguridad jurídica quizás hasta en cadenas de valor más complejas. En particular, cada agente de la cadena de valor que influya en la seguridad del producto y los usuarios (al modificar el producto) asumiría su responsabilidad y proporcionaría al siguiente agente de la cadena la información y las medidas necesarias.
2. Si los marcos de responsabilidad civil nacionales y de la Unión ven menoscabada su eficacia por las características de estas tecnologías digitales, algunas de las cuales pueden dificultar la relación causal entre los daños y un comportamiento humano, que es uno de los presupuestos para presentar una reclamación por responsabilidad subjetiva de acuerdo con las normas nacionales. La prueba puede resultar gravosa o excesivamente onerosa, de suerte que es posible que las víctimas no reciban una compensación adecuada, obteniendo una protección inferior a la que tienen respecto de otros productos o servicios similares. Será preciso valorar si las dificultades que estas tecnologías plantean para los marcos existentes podrían generar inseguridad jurídica en cuanto a cómo aplicar las normas en vigor (por ejemplo, cómo se aplicaría el concepto de culpa a los daños causados por la inteligencia artificial).

Se describen las siguientes dificultades y soluciones propuestas en este ámbito:

- a) Debe precisarse el ámbito de aplicación de la definición de «producto» de la Directiva sobre responsabilidad por productos defectuosos, de manera que refleje mejor la complejidad de las tecnologías emer-

gentes y garantice una adecuada indemnización por los daños y perjuicios causados por productos defectuosos debido a sus programas informáticos u otras características digitales.

- b) Debería contemplarse la posibilidad de adaptar las leyes nacionales para facilitar la carga de la prueba de las víctimas de daños causados por el uso de la inteligencia artificial, ya sea reduciéndola ya sea invirtiéndola. También sería aconsejable facilitar la carga de la prueba de las víctimas con arreglo a la Directiva sobre responsabilidad por los daños causados por productos defectuosos, de acuerdo con la cual un producto que no cumple con las medidas de seguridad obligatorias se considera defectuoso, con independencia de la culpa de los productores.
- c) Las dificultades que plantean la autonomía y la opacidad en las normativas nacionales sobre responsabilidad civil podrían resolverse siguiendo un enfoque basado en el riesgo. Los regímenes de responsabilidad civil subjetiva pueden garantizar que, siempre que se materialice dicho riesgo, la víctima sea indemnizada con independencia de que exista o no culpa, si bien deben ponderarse las consecuencias de la elección de quién debe ser el responsable civil objetivo de las operaciones de desarrollo y asimilación de la inteligencia artificial y debe así mismo considerarse un enfoque basado en el riesgo.

La responsabilidad por los daños derivados del uso de la inteligencia artificial fue también el centro de atención en la *Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones “Generar confianza en la Inteligencia artificial centrada en el ser humano (Building Trust in Human-Centric Artificial Intelligence)”*³⁶. De acuerdo con la Comisión, deben instaurarse mecanismos que garanticen la responsabilidad y la rendición de cuentas de los sistemas de inteligencia artificial y de sus resultados, tanto antes como después de su implementación. La posibilidad de auditar estos sistemas por parte de auditores internos y externos es fundamental, pues ello, junto a la disponibilidad de los informes de evaluación, contribuye en gran medida a la fiabilidad de la tecnología. La posibilidad de realizar auditorías externas debería garantizarse especialmente en aplicaciones que afecten a los derechos fundamentales (por ejemplo, las aplicaciones críticas para la seguridad)³⁷.

Entre las líneas de acción a implementar antes del tercer trimestre del 2019 con el objetivo de garantizar el desarrollo ético de la Inteligencia artificial en Europa en su

³⁶ Bruselas 8 de abril de 2019, COM(2019)168 final.

³⁷ *Directrices para una Inteligencia artificial fiable elaboradas por el Grupo de Expertos de Alto Nivel sobre la Inteligencia artificial*, apartado 2.1, 7º.

contexto más amplio, la Comunicación citada incluye la elaboración de un Informe sobre los retos que plantea la inteligencia artificial en relación con la seguridad y la responsabilidad y un documento de orientación sobre la implementación de la Directiva sobre responsabilidad por los daños causados por productos defectuosos. Pues bien, en noviembre de 2019 se publicó el *Informe sobre responsabilidad derivada de la inteligencia artificial y otras tecnologías digitales emergentes (Liability for Artificial Intelligence and other emergin digital Technologies)*³⁸ del Grupo de Expertos sobre Responsabilidad y Nuevas Tecnologías de la Comisión Europea, de acuerdo con el cual la tecnología digital genera nuevos riesgos que imponen la adopción de la regulación sobre responsabilidad de todo tipo (civil, administrativa y penal) para proteger a las víctimas. La normativa sobre seguridad de los productos, si bien otorga una protección básica a los perjudicados por el uso de las tecnologías digitales, no les garantiza la obtención de una compensación adecuada, principalmente, porque las regulaciones parten de los regímenes de responsabilidad civil de derecho privado (en particular, el derecho extracontractual), frecuentemente en combinación con el seguro. Por ello, considera que debe construirse una regulación común en la Unión Europea, porque sólo un régimen de responsabilidad estricta de los productores por productos defectuosos está armonizada a nivel europeo por la Directiva sobre responsabilidad del producto, mientras que los demás regímenes, aparte de algunas excepciones en sectores específicos o bajo legislación especial, están regulados por cada Estado Miembro. El Informe concluye que los actuales regímenes de responsabilidad de los Estados Miembros ya garantizan una protección básica a las víctimas de los daños causados en el uso de las tecnologías digitales, si bien, sus características específicas y aplicaciones pueden dificultar la indemnización en todos los casos en que la misma parezca justificada e incluso puede ocurrir que la asignación de responsabilidad sea injusta o ineficiente. Por ello incide en la necesidad de perfilar un régimen de daños específico para este tipo de situaciones, bien adaptando las normas actuales, bien creando un marco regulatorio específico que se base en las siguientes normas básicas³⁹:

1. Toda persona que utilice una tecnología digital cuyo uso comporte riesgos (por ejemplo, robots impulsados por inteligencia artificial en espacios pú-

³⁸ Supone la primera aproximación, a instancia comunitarias, al estudio de la responsabilidad por daños causados de accidentes provocados por tecnologías basadas en inteligencia artificial. Este documento continúa la línea de investigación iniciada por el Grupo de Expertos de Alto Nivel sobre Inteligencia artificial (High-Level Expert Group on Artificial Intelligence, AI HLEG) que en diciembre de 2018 publicó un Borrador de Directrices Éticas para el desarrollo y uso de la inteligencia artificial (Draft Ethics Guidelines for Trustworthy AI), en el que ya se anunció la necesidad de estudiar el régimen de responsabilidad aplicable a los productos basados en inteligencia artificial.

³⁹ Vide BARJOLA, J.M. y FERNÁNDEZ, C.B.: *Propuesta para un régimen de responsabilidad por uso de la Inteligencia artificial en la Unión Europea*, Diario La Ley 3 de diciembre de 2019, <https://diariolaley.laleynext.es/dll/2019/12/03/propuesta-para-un-regimen-de-responsabilidad-por-uso-de-la-inteligencia-artificial-en-la-union-europea>.

blicos) debe estar sujeta a requisitos estrictos de responsabilidad por daños. En caso contrario, es decir, si se trata de tecnologías cuyo uso no comporte riesgos, el usuario deberá cumplir con los deberes de seleccionar, operar, verificar y mantener adecuadamente la tecnología en uso y, en su defecto, responderá por el incumplimiento de tales deberes si es culpable del daño causado.

2. El sujeto que utilice una tecnología digital con cierto grado de autonomía, deberá responder por los daños causados del mismo modo que si éstos hubieran sido ocasionados por un auxiliar humano.
3. Los fabricantes de productos o contenidos digitales deben responder por los daños causados por sus defectos, incluso si los mismos fueron ocasionados por los cambios realizados en aquéllos bajo el control del productor tras haber sido colocados en el mercado.
4. Cuando el uso de las tecnologías exponga a terceros a un riesgo incrementado de daños, un seguro de responsabilidad civil obligatorio podría mejorar el acceso de las víctimas a la compensación y proteger a los potenciales causantes contra el riesgo de la responsabilidad.
5. Debe facilitarse la prueba de un elemento de la responsabilidad cuando la tecnología lo dificulta.
6. Las tecnologías digitales emergentes deben incorporar funciones de registro, de suerte que la falta de registro o de un acceso razonable a los datos registrados debe dar lugar a una inversión de la carga de la prueba para no perjudicar a la víctima.
7. La destrucción de los datos de la víctima debe considerarse como un daño específico compensable bajo condiciones propias.
8. No es preciso dotar a los dispositivos o sistemas autónomos de una personalidad jurídica propia, ya que el daño que pueden causar debe ser imputable a una persona o entidad preexistente.

3.2. Estado actual de la cuestión

El 20 de octubre de 2020 el Parlamento Europeo aprobó tres Informes que analizan cómo reglamentar la inteligencia artificial para promover la confianza en esta tecnología, la innovación y el respecto de estándares éticos:

1. Un Proyecto de Informe centrado en las cuestiones éticas (presentado por el eurodiputado español Ibán García del Blanco el 8 de octubre de 2020), basado en la garantía de la seguridad, la transparencia y la responsabili-

dad para evitar cualquier forma de sesgo y de discriminación, así como en el respeto de los derechos fundamentales. Cualquier ley futura, se afirma, deberá atenerse a los siguientes principios: una inteligencia artificial antropocéntrica y antropogénica; seguridad, transparencia y rendición de cuentas; salvaguardas contra el sesgo y la discriminación; derecho de reparación; responsabilidad social y medioambiental; respecto a la intimidad; y protección de datos.

2. Un Informe dedicado a la responsabilidad civil (*Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL), presentado por el eurodiputado alemán Axel Voss el 5 de octubre de 2020) que alienta la promoción de normas de la Unión en esta materia a escala internacional y cuyo objetivo es generar confianza al proteger a los ciudadanos, promover la innovación y garantizar la seguridad jurídica a las empresas. En el Anexo a la Propuesta de Resolución se incluyen *Recomendaciones para la elaboración de un Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial*.

Su contenido puede sintetizarse del siguiente modo:

- a) En cuanto a si es necesario un nuevo marco jurídico o basta con actualizar el existente, el Parlamento Europeo estima que no es precisa una revisión completa de los regímenes de responsabilidad civil, bastando con llevar a cabo una serie de ajustes precisos específicos que eviten que las víctimas se vean privadas de la correspondiente indemnización. Se considera fundamental una legislación uniforme que evite la fragmentación normativa en la Unión; si bien son preferibles reglamentaciones sectoriales específicas para la amplia gama de posibles aplicaciones, parece necesario contar con un marco jurídico horizontal y armonizado basado en principios comunes con el fin de garantizar la seguridad jurídica, establecer una igualdad de normas en toda la Unión y proteger eficazmente los valores europeos y los derechos de los ciudadanos.
- b) Entiende que debe revisarse la Directiva sobre responsabilidad por los daños causados por productos defectuosos, que será aplicable en relación con las reclamaciones por responsabilidad civil presentadas contra el productor de un sistema de inteligencia artificial defectuoso. Debe evaluarse si es necesario transformar dicha Directiva en Reglamento, es necesario aclarar la definición de «producto» de suerte que abarque los contenidos y servicios digitales, urge la adaptación de conceptos como los de «daño», «defecto» y «productor» y resulta

más que aconsejable revertir las normas que rigen la carga de la prueba en casos claramente definidos y tras una adecuada evaluación.

- c) Rechaza de plano el reconocimiento de personalidad jurídica y conciencia humana a los sistemas dotados de inteligencia artificial, por considerar que los daños que su uso haya podido causar casi siempre son resultado de que alguien ha construido o implantado los sistemas o intervenido en ellos; su única tarea es servir a la humanidad. Los modernos sistemas de inteligencia artificial tienen, por lo general, un funcionamiento más bien trivial y distan mucho de los robots conscientes que conocemos a través de las películas de ciencia ficción, de manera que cualquier debate sobre dotarles de personalidad jurídica está obsoleto. Las dificultades que pudieran derivarse de las características de estas tecnologías pueden dificultar la determinación de la intervención humana causante del daño, más dichas dificultades pueden salvarse haciendo responsables a todas las personas de toda la cadena de valor que crean, mantienen o controlan el riesgo asociado al sistema de inteligencia artificial.
- d) La legislación vigente de los Estados Miembros en materia de responsabilidad subjetiva ofrece un nivel de protección suficiente a las personas afectadas por un tercero interviniente (pirata informático), ya que como regla general dicha intervención constituye una acción de responsabilidad subjetiva en la que el tercero usa el sistema de inteligencia artificial para causar daños. Sólo en casos específicos, incluidos aquellos en los que el tercero no sea rastreable o sea insolvente, es necesario añadir normas para completar los marcos nacionales.

Por ello el Informe se centra en las reclamaciones de responsabilidad civil contra el operador de un sistema de inteligencia artificial, que se justifica por el hecho de que controla un riesgo asociado al sistema comparable al del propietario de un automóvil.

Aclara que debe entenderse por «operador» tanto el operador inicial⁴⁰ como el operador final⁴¹, siempre que este último no esté cubierto por la Directiva sobre responsabilidad por los daños causados por productos defectuosos.

⁴⁰ Persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema y se beneficia de su funcionamiento.

⁴¹ Persona física o jurídica que define, de forma continuada, las características de la tecnología, proporciona datos y un servicio de apoyo final de base esencial y, por lo tanto, ejerce también un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de inteligencia artificial.

Sostiene que todos los operadores, si intervienen varios, deben ser responsables civiles solidarios, si bien les reconoce derecho a recurrir unos contra los demás de forma proporcional. Los porcentajes de responsabilidad vendrán determinados por los respectivos niveles de control que tengan sobre el riesgo relacionado con la operación y el funcionamiento del sistema. A efectos de mejorar la identificación de los intervinientes en las distintas fases, debe mejorarse la trazabilidad de los productos.

No es admisible que el operador argumente que la actividad, el dispositivo o el proceso físico o virtual que causa el daño se encontraba fuera de su control debido a que fue causado por un funcionamiento autónomo. Todo sujeto que crea o mantiene un riesgo para el público es responsable si dicho riesgo causa un daño y, por consiguiente, debe minimizar *ex ante* o indemnizar *ex post* dicho riesgo.

- e) Para los sistemas de inteligencia artificial autónomos de alto riesgo⁴² es razonable establecer un régimen común de responsabilidad objetiva o basado en el riesgo. El Parlamento Europeo afirma que estos sistemas deben quedar exhaustivamente enumerados en un Anexo al Reglamento. Los demás sistemas que ocasionen daños que no estén incluidos en el citado Anexo quedarán sujetos a la responsabilidad subjetiva, permitiéndose al afectado acogerse a una presunción de culpa del operador y a los operadores la posibilidad de exculparte demostrando su actuación diligente. Ello salvo que se trate de robots que hayan causado incidentes reiterados que dan lugar a un daño o perjuicio grave, en cuyo caso los operadores deberán quedar sujetos a una responsabilidad objetiva; en estas hipótesis, la Comisión deberá valorar su inclusión en el Anexo, considerándose ésta con efecto retroactivo desde el momento del primer incidente probado. La Comisión deberá revisar el Anexo en el plazo más breve posible y en todo caso cada 6 meses y, si procede, deberá modificarlo. No obstante, seguirán siendo aplicables a aquéllos las legislaciones nacionales en relación con el importe y el alcance de la indemnización y con el plazo prescriptivo.
- f) Los operadores de los sistemas de inteligencia artificial de alto riesgo deberían ser titulares de un seguro de responsabilidad civil que cubra los importes y el alcance de la indemnización que se señale, sin

⁴² Se considera que un sistema de inteligencia artificial presenta un alto riesgo cuando su funcionamiento autónomo conlleva un potencial significativo de causar daño a una o más personas, de forma aleatoria y yendo más allá de lo que razonablemente cabe esperar.

que las primas sean tan elevadas que obstaculicen la investigación y la innovación. Debe alentarse a los Estados Miembros para que, en casos excepcionales (como por ejemplo cuando se produzcan daños colectivos) en los que la indemnización exceda significativamente de los importes máximos que se establezcan en el Reglamento, creen un fondo especial de indemnización para un período de tiempo limitado que responda a las necesidades específicas de tales supuestos. También podrían crear fondos especiales de indemnización para cubrir los casos excepcionales en los que un sistema de inteligencia artificial que aún no esté clasificado como de alto riesgo y que en consecuencia no esté asegurado cause daños o perjuicios. Los mecanismos de indemnización financiados con fondos públicos no son una respuesta adecuada al auge de la inteligencia artificial, ya que impondrían una carga financiera innecesaria a los contribuyentes.

- g) Si el usuario participara en el incidente que causa el daño, debería ser considerado responsable si puede definirse como operador en virtud del Reglamento; en caso contrario, podrá incurrir en responsabilidad subjetiva.
- h) El Reglamento debe cubrir los daños o perjuicios a la vida, a la salud, a la integridad física, a la propiedad y los daños morales significativos que den lugar a un menoscabo objetivo y demostrable de los intereses personales y a una pérdida económica verificable por encima de un umbral.

Los sistemas de inteligencia artificial pueden causar también daños a los derechos personales y a otros intereses importantes jurídicamente protegidos, pero estas infracciones están ya contempladas en las disposiciones jurídicas ya existentes en estos ámbitos (por ejemplo, legislación contra la discriminación y legislación en materia de protección de los consumidores). Por ello no se han incorporado el uso de datos biométricos o de técnicas de reconocimiento facial por sistemas de inteligencia artificial; todo uso no autorizado en este ámbito ya está contemplado en legislaciones de protección de datos específicas, como el Reglamento General de Protección de Datos (RGPD).

- i) Debe fijarse el importe de la indemnización y su alcance⁴³, así como el plazo prescriptivo para la presentación de demandas sobre responsabilidad civil.

⁴³ El importe de la indemnización debe ser inferior significativamente al establecido en la Directiva sobre responsabilidad por los daños causados por productos defectuosos y ello porque el Reglamento propuesto sólo se refiere al daño o perjuicio de una sola persona resultante de una única utilización de un sistema de inteligencia artificial, mientras que la Directiva se refiere a una serie de productos o incluso a una línea de productos con el mismo defecto.

Se proponen los siguientes importes máximos de indemnización:

- En caso de fallecimiento, daños a la salud o a la integridad física: 2.000.000 Euros.

Cuando se producen daños físicos seguidos de la muerte, la indemnización se calculará sobre la base de los costes del tratamiento médico que hubiera seguido la persona antes de su muerte, así como del perjuicio económico experimentado por éste con carácter previo y la interrupción o la reducción de su capacidad para generar ingresos o el aumento de sus necesidades. Si la víctima tenía la obligación legal de apoyar a un tercero, el operador responsable deberá también indemnizar a éste tercero con el pago de una pensión alimenticia proporcional a la que la víctima hubiera debido pagar durante un período equivalente a la esperanza de vida media de una persona de su edad teniendo en cuenta su estado de salud. También deberá indemnizar al tercero si al tiempo del fallecimiento de la víctima aquél estaba ya concebido pero no nacido.

En los casos de daños a la salud o a la integridad física la indemnización incluirá el reembolso de los gastos del tratamiento médico correspondiente, el pago del perjuicio económico sufrido por la suspensión temporal, la reducción o la interrupción definitiva de su capacidad para generar ingresos o del aumento consiguiente de sus necesidades acreditado mediante certificado médico.

- En caso de daños morales significativos que generen una pérdida económica verificable o daños en la propiedad y cuando distintos bienes propiedad de una persona afectada resulten dañados como consecuencia de una única utilización de un único sistema de inteligencia artificial de alto riesgo: 1.000.000 Euros.

Cuando la indemnización combinada que deba abonarse a varias personas que sufran daños o perjuicios supere estos importes máximos, los importes que deban abonarse a cada perjudicado se reducirán proporcionalmente hasta que la indemnización combinada no supere dichos límites.

Se proponen como plazos prescriptivos los siguientes, sin perjuicio de la legislación nacional que regule la suspensión y la interrupción de los mismos:

- En los casos de daños a la vida, a la salud o a la integridad física, 30 años a contar desde que se produjo el daño.
- En el caso de daños materiales o morales considerables: 10 años desde la fecha del menoscabo patrimonial o la pérdida económica verificable del daño moral, o 30 años desde que tuvo lugar la operación del sistema de inteligencia artificial de alto riesgo que causó posteriormente el menoscabo al patrimonio o el daño moral.

De estos plazos se contemplará el que antes venza.

- j) Recomienda los siguientes principios orientadores de la propuesta solicitada⁴⁴:
- Armonización total mediante un Reglamento en aras de un mercado digital único genuino.
 - Garantía de la máxima seguridad jurídica a lo largo de toda la cadena de responsabilidad, en particular para el productor, el operador, la víctima y cualquier otro tercero.
 - Debe evitarse una soberregulación, que obstaculizaría la innovación y el desarrollo.
 - Lograr un equilibrio entre la protección del público y los incentivos empresariales para invertir en innovación.
 - Deben configurarse como pilares básicos del marco común la propuesta de Reglamento y la Directiva sobre responsabilidad por los daños causados por productos defectuosos.
 - Los ciudadanos deben tener derecho al mismo nivel de protección y de derechos con independencia de que el daño sea o no causado por un sistema de inteligencia artificial, físico o virtual.
 - Debe tenerse en cuenta tanto el daño material como el inmaterial.

⁴⁴ Anexo a la Propuesta de Resolución: Recomendaciones para la elaboración de un Reglamento del Parlamento Europeo y del Consejo relativa a la Responsabilidad civil por el funcionamiento de los sistemas de Inteligencia artificial.

3. Un Informe centrado en los Derechos de Propiedad Intelectual (*Informe sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial* (2020/2015(INL), firmado por el eurodiputado francés Stéphane Séjourné el 2 de octubre de 2020), que enfatiza la importancia de un sistema efectivo que permita el desarrollo de la inteligencia artificial y con ello el registro de patentes y los nuevos procesos creativos.

Se destaca que la Comisión no ha abordado el problema de la protección de los derechos de propiedad intelectual en el contexto del desarrollo de la inteligencia artificial y las tecnologías diversas, razón por la cual solicita que se efectúe una evaluación de impacto respecto de la protección de dichos derechos en el contexto del desarrollo de estas tecnologías. Sugiere que la evaluación se centre en el impacto y en las implicaciones de la inteligencia artificial y las tecnologías conexas en el marco del actual régimen en materia de derecho de patentes, protección de marcas, dibujos y modelos, derechos de autor y derechos afines, incluida la aplicabilidad de la protección jurídica de las bases de datos y los programas informáticos, así como la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícita.

El Informe se pronuncia sobre tres cuestiones concretas: la necesidad de revisar el derecho de patentes europeo a la luz del desarrollo de la inteligencia artificial, la revisión de los derechos de propiedad intelectual en el ámbito del derecho europeo y el intercambio de datos creados en la Unión Europea para estimular la innovación en materia de inteligencia artificial.

En su Exposición de Motivos indica que debe preverse una evaluación del Derecho de patentes a la luz del desarrollo de la inteligencia artificial. Destaca que la patente protege las invenciones técnicas y, si bien los algoritmos, los métodos matemáticos y los programas de ordenador no son patentables en cuanto tales, pueden no obstante incluirse en una invención técnica susceptible de ser patentada; entiende que, si bien los modelos estadísticos y algoritmos computacionales en que se basa la inteligencia artificial no pueden patentarse en cuanto tales por contemplarse como métodos matemáticos en el sentido del Convenio sobre la Patente Europea (CPE), los métodos matemáticos y los programas informáticos pueden ser protegidos mediante patentes en virtud del artículo 52, apartado 3 de dicho Convenio cuando se utilicen como parte de un sistema de inteligencia artificial que contribuya a producir un efecto técnico suplementario, aunque reconoce que deberá evaluarse de forma minuciosa el impacto de dicha potencial protección de las patentes.

Se recuerda que el derecho de patentes exige una descripción exhaustiva de la tecnología subyacente, lo que puede conllevar dificultades de comprobación legal en el caso de determinadas invenciones basadas en tecnologías de inteligencia artificial, dada la complejidad de los razonamientos incorporados en ella.

También se destaca que la inteligencia artificial y las tecnologías conexas se basan en la creación y ejecución de programas informáticos que, como tales, están sujetos a un régimen específico de protección de los derechos de autor, por el cual la expresión de un programa informático puede ser protegida y no las ideas, los métodos y los principios subyacentes a cualquiera de sus elementos.

Se resalta la importancia de diferenciar entre las creaciones humanas con ayuda de la inteligencia artificial y las creaciones generadas por ésta de forma autónoma, puesto que estas últimas plantean nuevos retos normativos en materia de protección de los derechos de propiedad intelectual, como cuestiones sobre titularidad, la condición de inventor y la remuneración adecuada y otras relacionadas con la posible concentración del mercado. Subraya que a las primeras, en cambio, seguirá siendo aplicable el marco actual de derechos de propiedad intelectual.

Se indica que el presupuesto de la originalidad (unido a una persona física) puede obstaculizar la protección de las obras generadas por inteligencia artificial, pero que esta condición está destinada a evolucionar hacia una visión objetiva que tiende a caracterizar una novedad relativa permitiendo distinguir las obras protegidas de las obras ya creadas. Se trata de reconocer que una creación generada por inteligencia artificial puede constituir una obra teniendo en cuenta el resultado creativo en lugar del proceso de creación. Además, se señala que la falta de protección de estas obras podría dejar a los intérpretes de las mismas sin derechos, puesto que la protección del régimen de derechos afines implica la existencia de un derecho de autor sobre la obra interpretada. Se propone evaluar la posibilidad de reconocer los derechos de autor sobre este tipo de obras a la persona física que la edite y la haga pública de forma lícita, siempre que el diseñador (o los diseñadores) de la tecnología subyacente no se oponga(n) a dicho uso. Ello sería consecuente con el régimen europeo de protección de los «datos obra»; estos datos pueden ser explotados como parte de los datos utilizados para el entrenamiento de tecnologías de inteligencia artificial que generan creaciones secundarias, incluso con fines comerciales, siempre que dicho uso no haya sido expresamente reservado por sus titulares de derechos.

El informe también hace hincapié en la importancia de fomentar el intercambio de datos creados en la Unión Europea y en la necesidad de evaluar si las normas comunitarias sobre propiedad intelectual constituyen una herramienta adecuada para proteger su compilación, incluidos los datos sectoriales necesarios para el desarrollo de la inteligencia artificial.

Por último, el documento destaca el papel fundamental que deben jugar las personas y la revisión humana en los procedimientos de solicitud de concesión de derechos de propiedad intelectual, en la determinación de la responsabilidad en situaciones de infracción de dichos derechos, en la programación de dispositivos que utilizan la inteligencia artificial, en la selección de los datos entrantes, así como en el ajuste de los resultados obtenidos.

4. CONCLUSIONES

El Informe sobre aspectos éticos tiene como objetivo asegurar una inteligencia artificial antropocéntrica en la Unión Europea; una inteligencia artificial que sitúe al ser humano en el centro y colabore en la mejora de la calidad de vida. Propone la elaboración de un marco jurídico de principios éticos que sean respetuosos con los valores y los derechos fundamentales de la Unión y que sean de obligado cumplimiento para los softwares, los algoritmos y los datos incluidos en la inteligencia artificial, en la robótica y en las tecnologías conexas. En este sentido, sostiene que las tecnologías que generen un riesgo elevado, porque por ejemplo sean capaces de aprender solas, deberán diseñarse de tal modo que permitan en cualquier momento la supervisión humana. Cuando se utilice una función que pudiera atentar gravemente contra los principios éticos y resultar peligrosa, las capacidades de autoaprendizaje deberán desactivarse y se deberá restaurar plenamente el control humano. El citado Informe se inspira, a este respecto, en el documento *Directrices Éticas para la inteligencia artificial de Confianza* publicado por el Grupo de Expertos de Alto Nivel sobre inteligencia artificial el 8 de abril de 2019, en el que se advierte que la inteligencia artificial únicamente será de confianza si es lícita, ética y robusta desde un punto de vista técnico y social y en el que se establecen los siguientes presupuestos a tales efectos: intervención y supervisión humana, robustez y seguridad, privacidad y gestión de datos, transparencia, diversidad, no discriminación y equidad, bienestar social y medioambiental y rendición de cuentas.

En materia de responsabilidad civil, la propuesta es plausible, ya que teniendo en cuenta los problemas que el uso de la inteligencia artificial puede generar y los enormes esfuerzos que la jurisprudencia tendrá que llevar a cabo para dar respuesta a los problemas de responsabilidad civil que con seguridad se van a plantear, es conveniente dotar a esta realidad de un marco propio y específico. Es precisa una normativa específica que regule la responsabilidad civil en los supuestos de daños causados

por sistemas de inteligencia artificial, que van a ir incrementando en el tiempo paralelamente a su uso; en palabras de HERNÁNDEZ ESTÉBAN, E., no basta con parchear la legislación vigente, sino que, al contrario, debe abordarse el tema de raíz⁴⁵.

Es loable la aclaración que se lleva a cabo de la cuestión conceptual; como se ha reiterado en diversas ocasiones, de ello depende el tema de la responsabilidad civil. Queda resuelta la duda que “traía de cabeza” a la doctrina sobre si debía considerarse a los robots como un objeto o como un producto que goza de mayor o de menor autonomía, en cuyo caso el resultado era la inimputabilidad del mismo, o como un agente o un sujeto autónomo con capacidad para ser titular de derechos y de obligaciones y, en consecuencia, imputable. Se rechaza el reconocimiento a los mismos de una «personalidad electrónica» en base a la carencia de conciencia, de libre albedrío más allá de sus correspondientes programaciones y de su propia capacidad para tomar decisiones autónomas basadas en su propio aprendizaje y de independencia⁴⁶; los robots son instrumentos o herramientas de las que se sirve el ser humano para la consecución de ciertos objetivos y que, de momento, operan en base a instrucciones programadas. Siempre van a pertenecer a personas (físicas o jurídicas) que serán las que, en última instancia, permitirán o decidirán que siga funcionando o no; no se les puede imputar responsabilidad porque partimos de una voluntad que no se forma de manera libre, sino en su condición de “ser” dependiente y sometido a la voluntad de otro⁴⁷.

Dentro de la inteligencia artificial se distingue entre la «inteligencia artificial débil», que existe cuando una máquina consigue resolver problemas para cuya solución los humanos precisan utilizar su inteligencia y la «inteligencia artificial fuerte» o «inteligencia artificial general», basada en redes neuronales artificiales y que, de momento, todavía no se ha logrado. El propio Parlamento Europeo, en la Exposición de Motivos del Informe sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la Inteligencia artificial (2020/2015 (INI)) pone de manifiesto que la perspectiva de una inteligencia artificial «fuerte», es decir, consciente de sí misma, parece extremadamente futurista. De hecho, si atendemos a las consideraciones de uno de los grandes expertos en inteligencia artificial, N.J. NILSON⁴⁸,

⁴⁵ *Inteligencia artificial y vehículos autónomos: el régimen de responsabilidad civil ante los nuevos retos tecnológicos*, Revista Aranzadi de Derecho y Nuevas Tecnologías, nº 48/2018 parte Cuestiones, BIB 2019\1541.

⁴⁶ En la actualidad, las máquinas dotadas de Inteligencia artificial están capacitadas para resolver problemas concretos y para realizar tareas específicas (DÍAZ-ALABART, S.: *Robots y responsabilidad civil*, Reus, Madrid, 2018, p. 14) y normalmente repetitivas.

⁴⁷ DÍAZ- LIMÓN, J.A.: *Daddy's car: La Inteligencia artificial como herramienta facilitadora de derechos de autor*, Revista La Propiedad Inmaterial, nº 22, Universidad Externado de Colombia, julio-diciembre 2016, DOI: <https://dx.doi.org/10.18601.165719.59.n22.06>, p. 97 y DE ANDRÉS, A.: *Robótica y responsabilidad*, Diario La Ley nº 40, sección Ciberderecho, 9 de junio de 2020, Wolters Kluwer, La Ley 5270/2020.

⁴⁸ *The Quest for Artificial Intelligence: a History of Ideas and Achievements*, Nueva York, Cambridge University Press, 2009.

para que veamos una inteligencia artificial de nivel humano tendremos que esperara unos años, en concreto valora que la misma llegará entre los años 2030 y 2100. Pues bien, sólo sería posible crear una personalidad jurídica específica en los supuestos de «robots dotados de inteligencia artificial fuerte», es decir, con relación a robots que sean capaces de imitar el total funcionamiento de la mente humana, incluyendo la capacidad resolutoria de tareas y los sentimientos, la creatividad y la autoconciencia. Y precisamente en este último tipo de inteligencia artificial pensaba la Resolución del Parlamento Europeo de 17 de febrero de 2017 cuando propuso, entre diversas soluciones, la de crear a largo plazo una personalidad jurídica específica para los robots, de manera que al menos los más complejos pudieran ser considerados personas electrónicas responsables de reparar los daños y perjuicios que puedan causar⁴⁹.

Se ha optado, por lo tanto, por la solución más coherente, que es la de atribuirles la condición de «cosa», tal y como hizo el *Dictamen del Comité Económico y Social Europeo sobre la inteligencia artificial: las consecuencias de la Inteligencia artificial para el mercado único (digital), el consumo, el empleo y la sociedad*⁵⁰, en el cual el Comité Económico y Social (CESE) se opuso a la atribución de personalidad jurídica a los sistemas dotados de inteligencia artificial y defendió un enfoque basado totalmente en el control humano, de suerte que las máquinas continúen siendo tales y los humanos conserven en todo momento su dominio sobre ellas⁵¹. En cualquier caso, debe advertirse que atribuirles personalidad no habría servido de absolutamente nada si al mismo tiempo no se les hubiera dotado de un patrimonio⁵². En toda acción de indemnización de daños y perjuicios hay un componente resarcitorio que precisa de un patrimonio sobre el que ejercer dicho resarcimiento, de manera que, para poder imputar y exigir responsabilidad a un sistema dotado de inteligencia artificial, además de configurarlo como causante autónomo y responsable del daño, debería ser titular de un patrimonio con el que la víctima se pudiera resarcir⁵³.

El interés por regular el impacto de la inteligencia artificial en el ámbito de la propiedad intelectual es igualmente plausible. Como ya reconociera el Parlamento

⁴⁹ Vide GONZÁLEZ GRANADO, J. *Derecho y robots en la Unión Europea. Hacia una persona electrónica*, disponible en <http://tallerdederechos.com/derecho-y-robots-en-la-union-europea-hacia-una-persona-electronica>.

⁵⁰ 526º Pleno del CESE de 31 de mayo y de 1 de junio de 2017, DOUE 31 de agosto de 2017.

⁵¹ NÚÑEZ ZORRILLA, C.: *Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la Inteligencia artificial*, Revista Española de Derecho Europeo nº 66/2018 parte Estudios, Pamplona, BIB 2018/9706.

⁵² ATAZ LÓPEZ, J.: Ob. Cit., p. 49; BARRIO ANDRÉS, M. (dir.): *Derecho de los Robots*, 2ª ed., Wolters Kluwer, 2019, pp. 107 a 109; DÍAZ-ALABART, S.: Ob. Cit., pp. 73 a 81 y ROGEL VIDE, C.: *Robots y personas*, en “Robots y el Derecho”, Coord. por ROGEL VIDE, C., Reus, 2018, pp. 7 a 23 y *Robots y personas*, Revista General de Legislación y Jurisprudencia, 2018-1, pp. 79 a 90.

⁵³ PLAZA PENADÉS, J.: *Protección y cuestiones legales de la inteligencia artificial*, Formación e-Learning, Curso de especialización en Know-How, propiedad intelectual e industrial en el mercado digital único digital, BIB 2019/4802, Editorial Aranzadi, enero de 2019.

Europeo en su Resolución de 16 de febrero de 2017⁵⁴, no existe ninguna disposición jurídica que se aplique específicamente a la robótica, pero las doctrinas y los regímenes actuales pueden aplicarse fácilmente a ésta, si bien algunos aspectos requieran especial consideración. La inteligencia artificial también genera cuestiones trascendentales en relación con la propiedad intelectual, principalmente la de determinar si las obras creadas por un sistema de inteligencia artificial son susceptibles de protección y con qué alcance, la de concretar si puede considerarse a dichos sistemas como autores y, en consecuencia, como titulares de los derechos de autor sobre esas obras y la de aclarar qué sucede con los derechos morales⁵⁵.

El debate jurídico a este respecto se abrió a partir de la publicación el 27 de enero de 2020 por parte de la Oficina Europea de Patentes (EPO) de dos Resoluciones⁵⁶ que denegaban dos solicitudes de patente europea⁵⁷ que designaban como inventor al sistema de inteligencia artificial DABUS⁵⁸, por considerar que la figura de inventor es incompatible con el concepto de inteligencia artificial. Para la resolución de estas solicitudes la EPO encargó un informe relativo a la autoría de las invenciones generadas mediante inteligencia artificial al Doctor Noam Shemtov (*Informe Shemtov*), de la Universidad Queen Mary de Londres, que publicó en febrero de 2019 y en el que afirmó que cualquier solicitud de patentes europea que designe como inventor a un sistema de inteligencia artificial debe ser denegada con arreglo al Convenio sobre la Patente Europea (o Convenio de Munich); dichos sistemas no cumplen con los requisitos consagrados por dicho Convenio para ser acreedores de una patente europea, puesto que al carecer de personalidad no puede ser propietaria de ningún bien, ni siquiera intangible, ni mantienen una relación laboral con un empleador o comitente. Como sostienen MONTEAGUDO MONEDERO, M. y GARCÍA PÉREZ, F.⁵⁹, si bien esta solución es ajustada y atinada conforme a la normativa vigente, es preciso un profundo debate y una homogeneización de criterios a nivel internacional que per-

⁵⁴ *Derechos de propiedad intelectual y flujo de datos*, 18.

⁵⁵ Vide MONTEAGUDO MONEDERO, M. y GARCÍA PÉREZ, F.: ¿Puede la *inteligencia artificial desarrollar una invención patentable?*, Actualidad Jurídica Aranzadi nº 958/2020, parte Comentario, BIB 2020\12246.

⁵⁶ Demandas nº 18 275 163.6 y 18 275 174.3.

⁵⁷ Una solicitud se refiere a un contenedor para comida que utiliza diseños fractales para generar hendiduras y bultos y la otra a una lámpara led diseñada para parpadear a un ritmo que imita las secuencias de la actividad neuronal en el proceso creativo de ideas, hecho éste que dificulta que la señal luminosa sea ignorada.

⁵⁸ DABUS es un sistema de Inteligencia artificial creado por Stephen Thaler, diseñado para identificar y desarrollar nuevos contenidos que, en su caso, podrían resolver problemas concretos. Conecta dos redes neuronales artificiales, una entrenada con conocimientos generales existentes en diversos campos y que, sobre esta base, genera nuevos contenidos y otra denominada «crítica» que controla a la primera para detectar aquellos contenidos que son realmente novedosos respecto a contenidos preexistentes.

⁵⁹ Ob. Cit.

mitan definir con claridad el concepto de inventor en los supuestos de invenciones autónomas de una inteligencia artificial.

Debe resolverse por tanto quién debe ser designado como inventor en los inventos “generados por la inteligencia artificial”. De momento, las Oficinas de patentes no pueden designar como tal al propio sistema de inteligencia artificial (inventor no humano) porque ello no se contempla en la legislación en materia de patentes. Deberían por consiguiente aclararse los conceptos de “invenciones generadas por la inteligencia artificial” de forma autónoma y de “invenciones generadas con la asistencia de la inteligencia artificial”; se trata de determinar cuándo la inteligencia artificial desarrolla una invención y cuándo opera como una mera herramienta, lo cual nos conduce inexorablemente al planteamiento de si esta tecnología tiene autonomía suficiente como para inventar, pues debe diferenciarse entre autonomía y automaticidad. No es lo mismo crear de forma autónoma, que crear merced a instrucciones que determinan las operaciones que se ejecutan⁶⁰.

En los tres Informes referidos se destaca la importancia de crear un marco jurídico operativo y plenamente armonizado en el ámbito de las tecnologías de inteligencia artificial que adopte la forma de un Reglamento (y no de una Directiva), con miras a evitar la fragmentación del mercado único digital europeo y a promover la innovación. La Comisión tiene previsto emitir su propuesta legislativa a principios del vigente año 2021; esperamos que así sea, dada la trascendencia de la materia y de sus distintas y múltiples implicaciones en una gran variedad de ámbitos, muchas de ellas, como ya se ha dicho, todavía inciertas.

BIBLIOGRAFÍA

Informes, resoluciones, comunicaciones y otras publicaciones consultadas

Proyecto de Informe con recomendaciones a la Comisión de normas de Derecho Civil sobre Robótica (2015/2013(INL), Ponente Mady Delvaux (S&D, Luxemburgo), 31 de mayo de 2016, PE582.443 01-00.

Informe con recomendaciones a la Comisión de normas de Derecho Civil sobre Robótica (2015/2013(INL), 27 de enero de 2017.

Resolución del Parlamento Europeo de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre Robótica (2015/2013 (INL).

Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *Inteligencia artificial para Europa*, COM(2018)237 final, Bruselas 25 de abril de 2018.

⁶⁰ Vide *Declaraciones por parte del Delegado de España (OEPM)* en “Diálogo de la OMPI sobre propiedad intelectual (PI) e Inteligencia artificial (IA), 4 de noviembre de 2020, disponible en https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/conversation_ip_ai/pdf/ms_spain.pdf.

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *Plan Coordinado sobre la inteligencia artificial*, COM(2018)795 final, Bruselas 4 de diciembre de 2018.
- Informe *Artificial Intelligence Index Report* 2019.
- Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre las *repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*, COM(2020)64 final y 65 final, Bruselas 19 de febrero de 2019.
- Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *Generar confianza en la Inteligencia artificial centrada en el ser humano* (Building Trust in Human-Centric Artificial Intelligence), COM(2019)168 final, Bruselas 8 de abril de 2019.
- Directrices éticas para la inteligencia artificial de confianza* publicado por el Grupo de Expertos de Alto nivel sobre Inteligencia artificial el 8 de abril de 2019
- Directrices para una inteligencia artificial fiable* elaboradas por el Grupo de Expertos de Alto Nivel sobre la Inteligencia artificial, 8 de noviembre de 2019.
- Informe sobre responsabilidad derivada de la inteligencia artificial y otras tecnologías digitales emergentes* (Liability for Artificial Intelligence and other emergin digital Technologies) del Grupo de Expertos sobre Responsabilidad y Nuevas Tecnologías de la Comisión Europea, 27 de noviembre de 2019.
- Libro Blanco sobre la inteligencia artificial -Un enfoque europeo orientado a la excelencia y la confianza*, (COM(2020)65 final), Bruselas, 19 de febrero de 2020.
- Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial, incluido en el *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL)), de 5 de octubre de 2020.
- Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL)), de 5 de octubre de 2020.
- Anexo a la Propuesta de Resolución: *Recomendaciones para la elaboración de un Reglamento del Parlamento Europeo y del Consejo relativa a la Responsabilidad civil por el funcionamiento de los sistemas de Inteligencia artificial*.
- Declaraciones por parte del Delegado de España (OEPM) en “Diálogo de la OMPI sobre propiedad intelectual (PI) e Inteligencia artificial (IA)”, 4 de noviembre de 2020, disponible en https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/conversation_ip_ai/pdf/ms_spain.pdf.

Monografías y artículos

- ATAZ LÓPEZ, J.: *Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial*, Working Papers, Universitat de Barcelona, Working Paper 4/2020, p. 18, texto que es una reproducción de un trabajo realizado en el marco del Proyecto de Investigación nº PGC2018-098206 B del Ministerio de Ciencia, Innovación y Universidades, titulado *El derecho de contratos en el entorno digital* y que ha sido previa-

- mente publicado como capítulo del Libro “Derecho de daños”, dir. por HERRADOR GUARDIA, Lefebvre 2020, pp. 317-375.
- BARJOLA, J.M. y FERNÁNDEZ, C.B.: *Propuesta para un régimen de responsabilidad por uso de la inteligencia artificial en la Unión Europea*, Diario La Ley 3 de diciembre de 2019, <https://diariolaley.laleynext.es/dll/2019/12/03/propuesta-para-un-regimen-de-responsabilidad-por-uso-de-la-inteligencia-artificial-en-la-union-europea>.
- BARRIO ANDRÉS, M. (dir.): *Derecho de los Robots*, 2ª ed., Wolters Kluwer, 2019.
- DE ANDRÉS, A.: *Robótica y responsabilidad*, Diario La Ley nº 40, sección Ciberderecho, 9 de junio de 2020, Wolters Kluwer, La Ley 5270/2020.
- DÍAZ-ALABART, S.: *Robots y responsabilidad civil*, Reus, Madrid, 2018.
- DÍAZ- LIMÓN, J.A.: *Daddy’s car: La inteligencia artificial como herramienta facilitadora de derechos de autor*, Revista La Propiedad Inmaterial, nº 22, Universidad Externado de Colombia, julio-diciembre 2016, DOI: <https://dx.doi.org/10.18601.165719.59.n22.06>
- GONZÁLEZ GRANADO, J. *Derecho y robots en la Unión Europea. Hacia una persona electrónica*, disponible en <http://tallerdederechos.com/derecho-y-robots-en-la-union-europea-hacia-una-persona-electronica>.
- HERNÁNDEZ ESTÉBAN, E.: *Inteligencia artificial y vehículos autónomos: el régimen de responsabilidad civil ante los nuevos retos tecnológicos*, Revista Aranzadi de Derecho y Nuevas Tecnologías, nº 48/2018 parte Cuestiones, BIB 2019\1541.
- MARTÍNEZ, D.: *¿Un mundo sin empleo humano?*, Actualidad Económica, Madrid, mayo 2017, <https://search.proquest.com>.
- MONTEAGUDO MONEDERO, M. y GARCÍA PÉREZ, F.: *¿Puede la inteligencia artificial desarrollar una invención patentable?*, Actualidad Jurídica Aranzadi nº 958/2020, parte Comentario, BIB 2020\12246.
- N.J. NILSON: *The Quest for Artificial Intelligence: a History of Ideas and Achievements*, Nueva York, Cambridge University Press, 2009.
- NÚÑEZ ZORRILLA, C.: *Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial*, Revista Española de Derecho Europeo nº 66/2018 parte Estudios, Pamplona, BIB 2018/9706.
- ORTIZ HERNÁNDEZ, S., GARROS FONT, I. y ROMERA SANTIAGO, M.: *Hacia la implantación de la inteligencia artificial en nuestro sistema judicial*, Revista Aranzadi Doctrinal nº 3/2020 parte Estudios, BIB 2020\8846.
- PLAZA PENADÉS, J.: *Protección y cuestiones legales de la inteligencia artificial*, Formación e-Learning. Curso de especialización en Know-How, propiedad intelectual e industrial en el mercado digital único digital, BIB 2019/4802, Editorial Aranzadi, enero de 2019.
- ROGEL VIDE, C.: *Robots y personas*, en “Robots y el Derecho”, Coord. por ROGEL VIDE, C., Reus, 2018, pp. 7 a 23 y Robots y personas, Revista General de Legislación y Jurisprudencia, 2018-1, pp. 79 a 90.
- SANCHEZ DEL CAMPO REDONET, A.: *Europa quiere regular a los robots*, Diario La Ley, nº 14, sección Ciberderecho, 28 de febrero de 2017, Ed. Wolters Kluwer, La Ley 2253/2017.