pensar
Revista de Ciências Jurídicas
e-ISSN:2317-2150
DOI: 10.5020/2317-2150.2018.8453

# Retos Regulatorios en torno a la Inteligencia Artificial

## *Desafios Regulatórios em torno da Inteligência Artificial*

## *Regulatory Challenges around Artificial Intelligence*

**Antonio Merchán Murillo***

**Resumen**

La inteligencia artificial se va abriendo paso. La magnitud del desafío es de talla mundial, motivo que está llevando a la UE a abordar los problemas jurídicos que se plantean. Este hecho nos permite plantear, de manera concreta, los retos que se presentan y las esferas que podrían necesitar un tratamiento jurídico uniforme, como objeto de contribuir al planteamiento de soluciones sistemáticas e internacionales, ya que los métodos tradicionales de regulación no son plenamente aplicables.

**Palabras clave:** Inteligencia artificial. Ética. Marco jurídico. Confianza. Responsabilidad.

***Resumo***

*A inteligência artificial está emergindo. A magnitude do desafio é de classe mundial, o que está levando a União Europeia (UE) a resolver os problemas jurídicos que surgem. Isto nos permite propor, concretamente, os desafios enfrentados e as áreas que podem precisar de um tratamento jurídico uniforme, a fim de contribuir para a abordagem de soluções sistemáticas e internacionais, já que os métodos tradicionais de regulação não são totalmente aplicáveis.*

***Palavras-chave:*** *Inteligência artificial. Ética. Marco jurídico. Confiança. Responsabilidade.*

***Abstract***

*Artificial intelligence is emerging. The magnitude of the challenge is world-class, which is leading the EU to address the legal problems that arise.This fact allows us to raise, in a concrete way, the challenges that arise and the areas that might need a uniform legal treatment, in order to contribute to the approach of systematic and international solutions, since the traditional methods of regulation are not fully applicable*

***Keyword:*** *Artificial intelligence. Ethics. Legal framework. Trust. Liability.*

## 1 Introducción

El rápido cambio tecnológico y su desarrollo han llevado a una era de tecnología y aplicaciones que nos están llevando a cambios transversales, fundado en los datos que nutren Internet. Este cambio se está llevando a cabo a través del Internet de las cosas (IoT), las comunicaciones máquina a máquina (m2m), la robótica, el big data o la inteligencia artificial (en delante, IA), centrándonos en esta última.

El motivo es que la inteligencia artificial contribuye muchísimo a la tendencia actual de automatización en la UE, denominada Industria 4.0. Se prevé que IA cambiará el funcionamiento económico de las empresas y tendrá un impacto enorme en la sociedad.

* Doctor por la Universidad de Sevilla. Profesor de Derecho Internacional Privado. Centro Universitario San Isidoro. Universidad Pablo de Olavide de Sevilla. Sevilla – Espanha. E-mail: amermur@gmail.com.

Nos encontramos ante una cuestión urgente según el análisis realizado por la Comisión Europea, que hace hincapié en las bazas de la industria digital europea, pero también expresa el temor de que el valor añadido se desplace masivamente de los agentes industriales hacia los propietarios de plataformas digitales privadas, y destaca la falta de normas comunes y soluciones interoperables (COMISIÓN EUROPEA, 2018, p. 2).

Es de vital importancia concienciar y fomentar una percepción común de los objetivos entre las empresas y todas las partes interesadas, a saber, los interlocutores sociales a todos los niveles, el mundo académico, los institutos de investigación, los agentes públicos regionales y locales, el sector educativo y los consumidores.

Los debates públicos recientes han girado especialmente en torno a la necesidad de regular la propia esfera de la IA y establecer límites, para evitar que se desarrolle la denominada inteligencia general artificial, es decir, un sistema inteligente comparable a la capacidad intelectual humana o incluso superior a ella. Además, los debates apuntan la necesidad de enseñar ética a los sistemas de inteligencia artificial e incluir en ellos los valores que reconoce la sociedad.

## 2 Necesidad de determinar una definición uniforme de inteligencia artificial

El término inteligencia artificial 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 (BUTTERWORTH, 2018, p. 259). Los sistemas basados en la IA, como indica la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, pueden consistir

> simplemente en un programa informático (p. ej. Asistentes de voz, programas de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware (p. ej. robots avanzados, automóviles autónomos, drones o aplicaciones del internet de las cosas). (PARLAMENTO EUROPEO, 2017).

Se utiliza la IA diariamente, por ejemplo, para traducir de un idioma a otro, generar subtítulos en los vídeos o bloquear el correo electrónico no solicitado (spam). Lejos de ser ciencia-ficción, la IA forma ya parte de nuestras vidas, en la utilización de un asistente personal para organizar nuestra jornada laboral, en el desplazamiento en un vehículo de conducción automática o en las canciones o restaurantes sugeridos por nuestros teléfonos.

Con la IA se trata de elaborar sistemas capaces de resolver problemas y desempeñar tareas mediante la simulación de procesos intelectuales. Se puede enseñar a la IA a resolver un problema, pero ella también puede estudiar el problema y aprender la manera de resolverlo por sí misma sin intervención humana. Los diferentes sistemas pueden alcanzar distintos niveles de autonomía y pueden actuar de modo independiente. En ese sentido, su funcionamiento y sus resultados son imprevisibles, ya que esos sistemas funcionan como “cajas negras” (CNUDMI/UNCITRAL, 2018, p. 2).

Hoy día existen diversas definiciones de inteligencia artificial (ČERKA; GRIGIENĖ; SIRBIKYTĖ, 2015, p. 382). Sin embargo, ninguna de ellas ha sido aceptada universalmente (CNUDMI/UNCITRAL, 2018, p. 1), hecho que nos lleva al primer reto, realizar una definición atemporal, general y, a la vez, robusta de IA, especialmente, cuando uno piensa en la regulación normativa de la misma.

No se puede regular una determinada cuestión sin establecer una definición sólida de lo que se regula. Por ello, resulta esencial establecer una definición generalmente aceptada de IA que sea común flexible y no lastre la innovación, teniendo en cuenta que la IA es cada vez más sofisticadas.

Pueden servir de punto de partida los principios que enunció la Cnudmi/Uncitral a la hora de establecer en sus Leyes Modelos sobre Comercio Electrónico o sobre Firma Electrónica los procedimientos y principios básicos, a la vez que fundamentales, para facilitar el empleo de las técnicas modernas de comunicación,

con objeto de consignar y comunicar la información en diversos tipos de circunstancias, tales como: la no discriminación, la neutralidad respecto de los medios técnicos y la equivalencia funcional. Estos principios están ampliamente reconocidos como elementos fundamentales del comercio electrónico (ILLESCAS, 2011, p. 31). Al mismo tiempo se ven reflejados en la enunciación de los requisitos que deben cumplir las comunicaciones electrónicas.

De esta forma, debe establecerse una definición europea común (PARLAMENTO EUROPEO, 2017), incluyendo las definiciones de sus subcategorías, teniendo en cuenta las siguientes características:

a) a capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos;

b) la capacidad de aprender a través de la experiencia y la interacción;

c) la forma del soporte físico del robot;

d) la capacidad de adaptar su comportamiento y acciones al entorno.

## 3 Retos éticos: evolución y vigencia

### *3.1 RoboLaw*

El proyecto RoboLaw fue un proyecto de dos años financiado por el 7º Programa Marco de la Comisión Europea para la Investigación y el Desarrollo Tecnológico. Se lanzó oficialmente en marzo de 2012, con el objetivo de evaluar si la regulación existente en la UE era suficiente para abordar los diversos problemas legales planteados por la tecnología robótica y así poder incentivar la innovación europea, en el sector de la robótica y la IA. Además, se evaluó la incidencia de la IA en los sistemas jurídicos nacionales y europeos, ante los nuevos desafíos a los derechos y libertades fundamentales que se planteaban.

El resultado más importante de RoboLaw fue un informe final que contiene las Directrices sobre la regulación de la robótica, que se presentó el 22 de septiembre de 2014 (PALMERINI et al., 2016, p. 80). Asimismo, debe indicarse que la Resolución del Parlamento Europeo sobre el Derecho civil europeo sobre robótica se basa en una serie de informes preparados en el marco de este proyecto.

RoboLaw destaca que la idea de describir los valores inscritos en los artefactos tecnológicos es el primer paso para iniciar una discusión sobre su significado moral y ético, así como para reflexionar sobre cómo deberían incluirse los valores específicos en el diseño de estos artefactos. Las cuatro aplicaciones robóticas seleccionadas fueron: automóviles automáticos, robots quirúrgicos, prótesis y robots de cuidado.

El análisis ético concluyó que el valor de la seguridad es importante, pero no es el único valor y, en algunos casos, puede no ser el más importante. Asimismo, se analizaron distintas cuestiones éticas para identificar los valores humanos y las áreas de la vida social que podían ser más vulnerables, tales como: los problemas de aceptación, seguridad y responsabilidad.

### *3.2 Planteamiento del debate: cuestiones a tener en cuenta para la regulación de la materia*

En nuestra opinión, debemos plantearnos una serie de cuestiones metodológicas y sustanciales de la regulación de la tecnología en general, y la robótica y la IA en particular. En primer lugar, cabe preguntarse si se pueden identificar argumentos suficientes para acomodar estas nuevas tecnologías, y por ello justificar un cambio en el marco legal existente; es decir, ¿son suficientes las leyes existentes para enfrentar los desafíos normativos de la tecnología y, de no ser así, algunas leyes deberían adaptarse para incluir la nueva tecnología, generalmente haciendo que el lenguaje de la Ley sea más neutral en materia de tecnología o más bien deberían ser leyes sui generis? Con la normativa administrativa existente, la falta de interoperabilidad está asegurada.

Como sabemos, la interoperabilidad es una cuestión de suma importancia. Cuando hablamos de ésta nos referimos a que los procesos, tecnologías y protocolos requeridos, para asegurar la integridad de

los datos y la identidad del ciudadano, cuando se transfieren de un sistema a otro, deberán conllevar, por definición, una correcta interconexión de los sistemas e intercambio de datos. Sin embargo, esta no siempre se lleva a cabo, pensemos en el derecho de acceso.

En el plano técnico, aunque abundan las normas, se ha de poner de relieve la falta de normas básicas comunes a algunas tecnologías. En el plano jurídico, las legislaciones, que prescriben una tecnología específica predominante, se señalan como factores, que impiden el progreso, la dificultad de los responsables en comprender sus respectivos marcos de confianza mutua e incluso en los temas de responsabilidad e indemnización (OCDE, 2005, p. 6). Un ejemplo, al problema de la interoperabilidad es y, a veces sigue siendo, la situación que está presente en España a nivel regional y en la UE: las autoridades estatales de toda Europa ofrecen acceso electrónico, centrándose, sobre todo, en las necesidades y medios nacionales, lo que ha generado un sistema complejo con soluciones diferentes, que ha provocado el nacimiento de nuevos obstáculos a los intercambios transfronterizos, que lastran el funcionamiento del mercado único para las empresas y los ciudadanos.

En segundo lugar, es necesario aclarar el papel directo e indirecto que la ética puede desempeñar en la regulación de la tecnología (LÓPEZ DE MANTARÁS, 2017, p. 49), en particular, ampliando el objeto del análisis del artefacto para incluir su uso e implicaciones morales para el contexto social, la forma en que se concibe y se diseña y, en última instancia, cómo da forma al conocimiento y la cultura democrática de la tecnología (GURKAYNAK; YILMAZA; HAKSEVERB, 2016, p. 752). Por otro lado, la discusión también debe dirigirse al tema de la mejora humana, pensemos, por ejemplo, en las laborales, las mejoras pueden conllevar la sustitución de miles puestos de trabajo.

Finalmente, resulta conveniente hacer hincapié en la necesidad de establecer consideraciones adicionales a la responsabilidad (BERTOLI, 2014, p. 33), no sólo a nivel nacional, sino internacional, ya que su uso está previsto, siempre, para algo más de lo que podamos pensar, entre ellos está uso comercial y la implicación de los datos. Empresas multinacionales ya piensa en el uso de los drones para entrega de mercancías, así como el uso de coches automáticos, etc.

### *3.3 La continuación del debate*

El impacto de la IA es transfronterizo. La UE está dando cuenta de ello, tratando de regular su esfera y establecer límites. Los debates apuntan a once áreas: ética, seguridad, privacidad, transparencia y rendición de cuentas, trabajo, educación y desarrollo de capacidades, desigualdad e inclusión, legislación y reglamentación; gobernanza y democracia, guerra, y superinteligencia (COMISIÓN EUROPEA, 2018, p. 2).

Estos debates están justificados y deben tenerse en cuenta. No obstante, son parte de un problema mayor, relacionado con la concepción insuficiente de la inteligencia artificial que tiene la sociedad, lo que dificulta la confianza, y con las leyes vigentes, que no han reconocido todavía las características específicas de la inteligencia artificial (CNUDMI/UNCITRAL, 2018, p. 1). De esta forma, surge la necesidad de analizar y profundizar en un marco ético para que tanto los ciudadanos como las empresas puedan confiar en la tecnología con la que interactúan, disponer de un entorno jurídico predecible y contar con la garantía efectiva de que van a protegerse sus derechos y libertades fundamentales.

Pensemos que las tecnologías basadas en la inteligencia artificial influyen en aspectos como la salud, la seguridad, la productividad o el ocio, y a medio plazo van a tener un gran impacto en la energía, el transporte, la educación y las actividades domésticas. Respecto a la educación resulta esencial encontrar nuevos modelos y metodologías que integren las preocupaciones éticas en relación con el impacto de la inteligencia artificial en la humanidad, especialmente en todo lo relacionado con la seguridad, la libertad, la intimidad, la integridad y la dignidad; la autodeterminación y la no discriminación, y la protección de los datos personales (PARLAMENTO EUROPEO, 2017, p. 5).

La complejidad de la IA conlleva la necesidad de crear un marco ético y eficiente, para ello debe partirse del principio de transparencia, que consiste en que siempre ha de ser posible justificar cualquier decisión que se haya adoptado con ayuda de la inteligencia artificial y que pueda tener un impacto significativo sobre

la vida de una o varias personas. Por otro lado, siempre debe ser posible reducir los cálculos del sistema de IA a una forma comprensible para los humanos.

En cualquier caso, es un debate candente. En el este aspecto destacan la Declaración de Barcelona para un desarrollo y uso adecuados de la inteligencia artificial en Europa, dictada con fecha 8 de marzo de 2017, momento en el que participaron diversos expertos en inteligencia artificial, computación y comunicación. El documento destaca seis puntos en el desarrollo y el uso de la inteligencia artificial (LÓPEZ DE MANTARÁS, 2017, p. 49):

1. La prudencia, la necesidad de ser conscientes de que todavía queda por resolver un gran número de obstáculos científicos y técnicos, en particular el problema del sentido común.
2. La fiabilidad, esto es, que los sistemas de inteligencia artificial deben someterse a pruebas que determinen su fiabilidad y seguridad.
3. La rendición de cuentas: cuando un sistema toma decisiones, las personas afectadas por ellas tienen que poder recibir, en unos términos de lenguaje que entiendan, una explicación de por qué las ha tomado, y tienen que poder cuestionarlas con argumentos razonados.
4. La responsabilidad, si la interacción se hace con una persona o con un sistema de inteligencia artificial, y, en el segundo caso, debe poderse localizar e identificar a los responsables de él.
5. La autonomía limitada de estos sistemas. Se necesita disponer de reglas claras que limiten el comportamiento de los sistemas de inteligencia artificial autónomos para que los encargados de desarrollarlos puedan incorporarlos en sus aplicaciones.
6. La claridad del papel que desempeña el ser humano. En casi cualquier área, la capacidad humana todavía supera con creces la inteligencia artificial, especialmente en el tratamiento de casos que no han aparecido en los conjuntos de datos de ejemplo de los que aprenden los sistemas de inteligencia artificial.

Observados los principios anteriores, uno de los que más llama la atención es el que se refiere a la autonomía, que nos puede llevar a preguntarnos si ¿puede una inteligencia artificial celebrar contratos vinculantes para su operador o propietario?; es decir, si una inteligencia artificial puede tomar decisiones independientes o puede interactuar con otras personas jurídicas sin el conocimiento de su operador o propietario. Entonces, ¿hasta qué punto ese operador o propietario debería ser responsable de las acciones de la inteligencia artificial?

En este extremo se presentan argumentos para crear a largo plazo una personalidad jurídica específica para los robots (ČERKA; GRIGIENĖ; SIRBIKYTĖ, 2017, p. 691), de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar y, posiblemente, aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente (PARLAMENTO EUROPEO, 2017, p. 17). En este punto, cualquier legislación que desarrolle dichos cambios requerirá una cuidadosa consideración de cómo una IA con personalidad jurídica se ajustaría a las leyes existentes y a la sociedad en su conjunto. Por otro lado, se presenta fundamental la confianza (COMISIÓN EUROPEA, 2018, p. 3). Los ciudadanos también necesitan comprender de qué modo funciona la tecnología, de ahí la importancia de la investigación sobre la explicabilidad de los sistemas de IA.

## 4 Marco normativo a falta de regulación directa

### *4.1. Protección de datos*

En términos de legislación existente, la protección de datos es actualmente el área clave de la Ley que se ocupa de los efectos de la IA en la sociedad. En este aspecto, destaca el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas

en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) que garantiza un elevado nivel de protección de los datos personales, e incluye los principios de protección de datos desde la fase de diseño y por defecto.

Asimismo, en el marco de la estrategia para el mercado único digital, la Comisión ha presentado una serie de propuestas que resultarán clave para el desarrollo de la IA, como el Reglamento sobre la libre circulación de datos no personales, y que reforzarán la confianza en el mundo en línea, como el Reglamento sobre la privacidad y las comunicaciones electrónicas y la Ley de ciberseguridad.

En cuanto a la protección de datos personales, el Reglamento supuso un paso de envergadura para reforzar la confianza, esencial tanto para las personas físicas como jurídicas. Ahora bien, algunas aplicaciones de la IA pueden plantear nuevos problemas en relación con la responsabilidad o la adopción de decisiones potencialmente sesgadas, por no quedar particularmente claras en este contexto regulatorio.

En este punto, deben tenerse claras las implicaciones en la protección de datos que llevan a la IA, en relación con los big data, para el análisis de los datos, que concretamente, desde nuestro punto de vista son: el uso de algoritmos (algoritmos de aprendizaje automático para analizar un conjunto de datos y luego extraer correlaciones para revertir el análisis de datos tradicional), opacidad del procesamiento (ciertos procesos algorítmicos operan como una “caja negra” para el usuario. En los algoritmos de procesamiento de datos tradicionales, habría un árbol de decisión y una lógica por la cual el algoritmo alcanzaría un rango de resultados establecidos); tendencia a recopilar datos (el aprendizaje automático necesita grandes conjuntos de datos para aprender, lo que significa que se recopila y analiza la mayor cantidad posible de datos); la reutilización de datos (por ejemplo, los datos generado a partir de una determinada actividad).

Con lo anterior, se observan ciertos riesgos en relación, por ejemplo, con el consentimiento manifestado de manera libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa (artículo 4,11), para el tratamiento de sus datos personales para uno o varios fines específicos (artículo 6,1-a), en tanto que puede obviarse una acción que requiera la autorización del usuario por conductas previas o anteriores de éste.

Asimismo, los riesgos de privacidad de la vinculación entre conjuntos de datos se vuelven particularmente graves cuando los sistemas de autenticación o los almacenes de datos tienen acceso a los datos que generan los dispositivos autenticados. Aunque ofrecen una mejor experiencia de usuario, el enlace y la personalización entre múltiples dispositivos y servicios de IA presentan riesgos para la privacidad del usuario.

Pensemos en los datos de las aplicaciones de salud o de aparatos como Fitbit que podrían, por ejemplo, ser relevantes para empresas al inferirse hábitos de ejercicio, comportamiento alimentario o sueño. La falta de sueño, que Fitbit rastrea, no cabe duda de que se puede relacionar con el bienestar: problemas de salud, bajo rendimiento cognitivo, emociones negativas como depresión, la tristeza, etc. Aparentemente, podría hablarse de datos aparentemente no personales, creados a través de la denominada anominización. No obstante, las deficiencias de la anonimización deben ser tenidas muy en cuenta; pues, existe una preocupación especial de que los datos vinculados a una determinada información pueden ser utilizados para predecir el comportamiento futuro. Asimismo, estos datos son susceptibles de abrirse a la reidentificación e ingeniería inversa de identidad, pensemos que la tecnología de la información permite a través de nodos y metadatos (big data) se vincule a un determinado dispositivo.

Estas preocupaciones quedan patentes en los artículos 21 y Artículo 22 RGPD. El artículo 21 introduce el derecho de oposición al procesamiento de datos, incluidos los perfiles, en cualquier momento. Si el propósito del procesamiento de datos es el marketing directo, el interesado tendrá derecho absoluto a oponerse. En todos los demás casos, el procesamiento de datos debe detenerse, a menos que el controlador de datos pueda demostrar intereses legítimos convincentes que anulen los intereses de los interesados. Por otro lado, el artículo 22 introduce salvaguardias adicionales contra la toma de decisiones automatizada, incluida la elaboración de perfiles, pero solo cuando el procesamiento de datos es únicamente automático y tiene efectos significativos legales o similares. Al mismo tiempo, lo que empieza siendo un dato no personal, al no identificar al individuo, es probable que la aplicabilidad de estos artículos sea muy limitada.

Normalmente, las partes intervienen en desigualdad de condiciones en los contratos realizados, siendo los principales riesgos de índole jurídica el desconocimiento de los puntos débiles inherentes a la tecnología que está siendo utilizada, las funciones de seguridad que faltan o son inadecuadas, así como los riesgos relacionados con los datos. De esta forma, podría preguntarse incluso si una persona está dando su consentimiento para un todo global o para un caso concreto general o un consentimiento en forma de nada.

Comunicar esta incertidumbre a los usuarios es un desafío pendiente y los riesgos deben ser analizados muy bien, pues estos van aparejados a una situación conflictiva de que los usuarios realicen una elección informada al establecer permisos de acceso socavan la protección real. La capacidad de los interesados para consentir libremente se verá aún más cuestionada si no pueden comprender el alcance, debido a la complejidad de las políticas de privacidad.

En relación con la protección de la privacidad y el consentimiento informado el artículo 25 RGPD crea un deber general en torno a la privacidad por defecto y la privacidad por mecanismos de diseño, lo que podría ayudar a resolver la incertidumbre del análisis invasivo de la privacidad y, por lo tanto, ofrecer una mejor base para el consentimiento informado. Si el usuario tiene la seguridad de que la privacidad estará protegida por defecto, el usuario puede tomar una decisión informada a medida que las posibles consecuencias de privacidad sean o no previsibles. Las medidas específicas requeridas dependerán de las circunstancias.

Otro punto ejemplo problemático sería el derecho al olvido (artículo 17); es decir, si el olvido tiene sentido para la IA, teniendo en cuenta que las máquinas no olvidan (VILLARONGA; KIESEBERG; LI, 2018, p. 305). Por ello, en nuestra opinión puede haber una clara desconexión entre el Reglamento y la realidad técnica, ya que debe observarse que hablamos de una tecnología basada en el procesamiento de datos. Algo parecido puede suceder en relación con la privacidad por diseño. La incapacidad de una máquina basada en IA para olvidar es obvia, pues hablamos de grandes bases de datos, donde la información anterior puede resultar esencial para otra. También cabría preguntarse, que conlleva para la propia IA en caso de que se borren esos datos.

### *4.2 Imputación de responsabilidad*

Hoy día existen iniciativas, informes o propuestas legislativas en Europa para considerar y abordar el impacto de la IA en la sociedad. Entre ellas destacan las propuestas de la Comisión Europea para que la UE desarrolle normas de derecho civil sobre el uso de robots y la inteligencia artificial (PARLAMENTO EUROPEO, 2017, p. 6), propuestas del "Artificial Intelligence Committee" de la Cámara de los Lores del Reino Unido, la última de ellas de 18 de abril de 2018 (ARTIFICIAL INTELLIGENCE COMMITTEE, 2018), el informe del gobierno británico sobre el crecimiento de la industria de inteligencia artificial en el Reino Unido (Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy, 2017) o iniciativas por parte del Gobierno de Estonia de que han comenzado a debatir la viabilidad y los marcos legales para la aplicación de las tecnologías de Inteligencia Artificial (PLANTERA, 2017, p. 1).

No obstante, las primeras Leyes vienen de EE. UU. que, por ejemplo, ha aprobado recientemente la primera ley del mundo para coches autónomos, demostrando que en Estados Unidos se están invirtiendo considerablemente en IA. Se trata de la Self Drive Act, aprobada con fecha 6 de septiembre de 2017, mediante la cual garantizar la seguridad de los vehículos altamente automatizados mediante el fomento de las pruebas y el despliegue de dichos vehículos. Además de esta Ley vendrán más para regular todos los sistemas conexos a la IA.

Ante esto, surge la necesidad de considerar que la responsabilidad civil por los daños y perjuicios causados por robots es una cuestión fundamental que también debe analizarse y abordarse, con el fin de garantizar el mismo grado de eficiencia, transparencia y coherencia en la garantía de la seguridad jurídica en toda la UE en beneficio de los ciudadanos, los consumidores y las empresas. Ante la complejidad de la asignación de responsabilidad por los daños y perjuicios causados por robots cada vez más autónomos, el Parlamento Europeo, en su Resolución, de 16 de febrero de 2017, con recomendaciones destinadas a la

Comisión sobre normas de Derecho civil sobre robótica, se considera partidario de crear a largo plazo una personalidad jurídica específica para los robots.

Al pensar sobre esta cuestión me resultó llamativo una noticia, de fecha 20 de abril de 2015, en la que representantes de la organización Non-Human Rights Project anuncian que, por primera vez en la historia, un juez, de la Supreme Court of the State of New York, County of New York, plantea la posibilidad de que dos chimpancés (Hércules y Leo) sean consideradas como personas jurídicas, lo que me llevó a preguntarme ¿y por qué no? No obstante, para responder a esta cuestión es necesario realizar un análisis filosófico profundo y legal del concepto de quien puede ser sujeto de derecho y obligaciones, de la misma forma que se hizo en su día, si se me permite el silogismo con el nasciturus (desde una perspectiva del Derecho Romano y su evolución a nuestros tiempos plasmándose en el Código Civil actual).

Dejando planteado lo anterior, cabe la posibilidad, al menos en teoría, de que se conciban futuras generaciones de sistemas automatizados de información con capacidad de funcionamiento autónomo, no simplemente automático. En otras palabras, es posible que, gracias a la evolución de la inteligencia artificial, una computadora pueda aprender de la experiencia, modificar las instrucciones que componen sus propios programas e incluso formular nuevas instrucciones.

De esta forma, desde un punto de vista técnico, puede resultar imposible justificar los motivos de una decisión concreta de inteligencia artificial. Por lo tanto, en caso de daños, las partes se encuentran en un vacío probatorio y pueden verse en la imposibilidad de determinar la responsabilidad al carecer de disposiciones específicas. La legislación debe establecer normas claras y equilibrar las obligaciones para proteger a ambas partes en un contrato y a los terceros que necesitan certidumbre sobre el ámbito en el que solicitar reparación por daños y perjuicios (ČERKA; GRIGIENĖ; SIRBIKYTĖ, 2017, p. 385). Dicho lo anterior, en la actualidad, debe tenerse en cuenta que la atribución a una persona física o jurídica de las acciones ejecutadas por un sistema automatizado de mensajes se basa en la idea de que los parámetros técnicos con que se programa un sistema circunscriben su capacidad de funcionamiento.

De esta forma, hoy en día, a falta de regulación legal directa de IA puede partirse, para determinar un marco jurídico concreto, del artículo 12 de la Convención de las Naciones Unidas sobre el Uso de Comunicaciones Electrónicas en Contratos Internacionales, que establece que una persona (ya sea una persona física o jurídica) en cuyo nombre se utilizó una computadora programado debería ser responsable de cualquier mensaje generado por la máquina. Ahora bien, en la nota explicativa, la Cnudmi deja claro que este artículo es una disposición habilitante y no debe entenderse erróneamente que transforma en sujeto de derechos y deberes un sistema automatizado de mensajes o una computadora. Debe interpretarse que las comunicaciones electrónicas que son generadas automáticamente por un sistema de mensajes o una computadora sin intervención humana “proceden” de la entidad jurídica en nombre de la cual funciona el sistema de mensajes o la computadora. Las cuestiones relativas al sujeto de la acción que podrían plantearse en ese contexto han de ser zanjadas con arreglo a normas al margen de la Convención, lo que nos vuelve a punto anterior (CNUDMI/UNCITRAL, 2007, p. 76-77).

### *4.3 El aspecto internacional como verdadero problema*

En este nuevo escenario tecnológico, en desarrollo constante a nivel nacional y, aún más, a nivel internacional, la protección de los derechos de las personas cobra un significado crucial, pues se trata de establecer garantías esenciales para generar confianza. En Internet puede haber realidad virtual, pero eso no significa que los derechos también lo sean: se trata de garantías expresas que deben quedar reconocidas en el ciberespacio.

#### *4.3.1 Respecto a la protección de datos*

Nadie puede sostener que los usuarios, por tratarse de Internet, pueden sufrir mengua de sus derechos. Este aspecto nos lleva a la protección de datos, cuya normativa siempre será aplicable con

independencia de la forma en que se generen, pues, como sabemos, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea dan cuenta de ello y establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Tal protección viene desarrollada por el Reglamento 2016/679 de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Este Reglamento en su artículo 79,2 determina la competencia judicial estableciendo, reglas que se aplican sobre las normas establecidas en el Reglamento 1215/2012 sobre competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Bruselas I), que "las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento", alternativamente tales acciones "podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad de un Estado miembro que actúe en ejercicio de sus poderes públicos" (CALVO; CARRASCOSA, 2018, p. 1363).

En cuanto a la determinación de la Ley aplicable, el Reglamento fija los casos en los que debe aplicarse, por razón del territorio en su artículo 3:

a) Establecimiento en la UE del responsable o del encargado, independientemente de que el tratamiento tenga lugar en la Unión. El criterio de conexión implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto (Considerando 22). Como puede observarse el lugar geográfico resulte irrelevante.

b) Residencia del interesado en la UE, si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago, por lo que debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión, y el control de su comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes. Por ejemplo, un responsable de fichero cuyo establecimiento se encuentra en los Estados Unidos recoge datos personales mediante programas de software espía que se instalan en el ordenador de los internautas que visitan ciertas páginas web desde España. Es preciso determinar la Ley aplicable a esta cuestión. A este caso cabría decir que, aunque el responsable del fichero tiene su sede fuera de la UE, el art. 3.2.b RGPD indica que este RGPD es aplicable al caso, pues las actividades de tratamiento están relacionadas con el control del comportamiento de una persona que reside en la UE cuyo establecimiento se encuentra en los Estados Unidos recoge datos personales mediante programas de software espía que se instalan en el ordenador de los internautas que visitan ciertas páginas web desde España. De esta forma, aunque el responsable del fichero tiene su sede fuera de la UE, el art. 3.2.b RGPD indica que este RGPD es aplicable al caso, pues las actividades de tratamiento están relacionadas con el control del comportamiento de una persona que reside en la UE.

c) Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro.

### *4.3.2 Respecto a los derechos de personalidad*

El Reglamento 1215/2012, de 12 de diciembre de 2012, en su considerando 16, se refiere a la necesidad, garantizar la seguridad jurídica y evitar la posibilidad de que una persona sea demandada ante un órgano jurisdiccional de un Estado miembro que no hubiera podido prever razonablemente. Este aspecto reviste particular importancia en relación con los litigios relativos a obligaciones no contractuales derivadas de vulneraciones del derecho a la intimidad y de los derechos de la personalidad, incluida la difamación (ÁLVAREZ, 2009, p. 82). La ausencia de un marco regulador global de las actividades informáticas en Internet, unida a la diversidad de normas de Derecho internacional privado previstas por los Estados, exponen a los medios a un marco jurídico fragmentado, pero también potencialmente contradictorio, pues aquello que se encuentra prohibido en un Estado podría, a su vez, estar permitido en otro (ESLAVA, 2014, p. 26).

Además, una información cualquiera que sea que se vuelque en la red, convierte a los particulares directamente, ya sea voluntaria o involuntariamente, en distribuidores de la información, a través de redes sociales. Por otra parte, las posibles víctimas de publicaciones lesivas de los derechos de la personalidad se encuentran en una posición de especial vulnerabilidad cuando el soporte es proporcionado por Internet. El titular del derecho de la personalidad afectado puede ser víctima, por tanto, de vulneraciones potencialmente más intensas, al tiempo que su tutela jurídica, dada la atomización e inseguridad jurídica que sufre, se ve disminuida (BOBEK, 2017, p. 104).

Lo anterior, se puso de manifiesto en la STJUE, de 25 de octubre de 2011, asuntos acumulados C-509/09 y C-161/10, caso *eDate*, que vino a determinar que la persona que se considera lesionada puede ejercitar una acción de responsabilidad por la totalidad del daño causado, bien ante los órganos jurisdiccionales del Estado miembro del lugar de establecimiento del emisor de esos contenidos, bien ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses. Esa persona puede también, en vez de ejercitar una acción de responsabilidad por la totalidad del daño causado, ejercitar su acción ante los tribunales de cada Estado miembro en cuyo territorio el contenido publicado en Internet sea, o haya sido, accesible. Dichos órganos son competentes únicamente para conocer del daño causado en el territorio del Estado miembro del órgano jurisdiccional al que se haya acudido.

Determinada la competencia conforme a lo anterior, cabe plantear la Ley aplicable. Las leyes españolas que regulan los derechos al honor, intimidad y propia imagen no contienen normas que conflicto de leyes que concreten la Ley estatal aplicable a estos derechos en los casos internacionales (CALVO; CARRASCOSA, 2018, p. 1363). Ante este hecho, han surgido varias tesis sobre cuál debe ser la Ley estatal reguladora de estos derechos (CARRASCOSA, 1997, p. 520): a) Sistema del estatuto personal; b) Sistema de responsabilidad civil no contractual; c) Sistema mixto entre los dos anteriores; d) Consideración de las normas relativas a los derechos de la personalidad como normas procesales; e) Sistema del derecho subjetivo; f) Consideración de las normas relativas a los derechos de la personalidad como normas materiales imperativas.

La tesis seguida por la mayoría de la doctrina es la del sistema de responsabilidad no contractual, determinándose como la ley aplicable a los derechos de la personalidad se fija mediante el art.10, 9-I C. C., que conduce a la Ley del país donde se ha producido la vulneración del derecho de la personalidad (GARAU, 1990, p. 420).

Ahora bien, para determinar el país donde se ha producido el daño, habrá de tenerse presente que las vulneraciones de los derechos de la personalidad se van a producir mediante una cadena de ilícitos. De esta forma, si el tratamiento de datos se desarrolla, como es frecuente, en distintas fases, recogida de datos, clasificación de estos, cesión a terceros de los datos, divulgación de estos, etc., cada acción se regirá por la Ley del país en cuyo territorio haya tenido lugar.

### *4.3.3 Desde un punto de visto contractual*

Las partes contratantes tienen que hacer frente a la incertidumbre en cuanto a la magnitud de la diligencia debida en lo que respecta a la elaboración de algoritmos o la posible responsabilidad por fallos en el funcionamiento del sistema, al tiempo que son incapaces de predecir comportamientos futuros y no

tienen ningún control sobre su utilización y el ingreso de datos en el futuro, que pueden afectar, de modo muy importante, al sistema de inteligencia artificial (CNUDMI/UNCITRAL, 2018, p. 4).

Obsérvese que la atribución legal de las transacciones realizadas por los sistemas de inteligencia artificial está clara, habida cuenta de que la tecnología de inteligencia artificial y los servicios basados en inteligencia artificial suelen implicar distintas jurisdicciones, las partes necesitan medios eficaces para proteger sus intereses.

Los sistemas de inteligencia artificial pueden considerarse agentes electrónicos mediante los cuales las partes celebran transacciones jurídicas y quedan obligadas por ellas. Sin embargo, algunas empresas pueden poner a prueba el ordenamiento jurídico creando aplicaciones de inteligencia artificial que actúan por sí mismas y tienen sus propios objetivos y propósitos mientras el autor permanece oculto. Y aún se producen situaciones más complicadas cuando la inteligencia artificial creada por otro sistema de inteligencia artificial interactúa con seres humanos. Hasta la fecha, no hay una solución jurídica satisfactoria.

Lo mismo se aplica a la responsabilidad extracontractual. En este sentido, puede ser particularmente difícil determinar las responsabilidades debido a la falta de pruebas, así como a la participación de varias personas cuya responsabilidad es difícil de dilucidar. Además, los seguros pueden no cubrir todas las situaciones en que se producen los daños.

A este respecto, en los países de la common law opinan que, en ciertas circunstancias, no todo lo acordado entre las partes está en el contrato y que, por lo tanto, algunas condiciones son implícitas, por lo que está cuestión estaría cubierta por la materia contractual, mientras que en los países de la civil law, la cuestión sería materia extracontractual.

Estos hechos ponen de manifiesto la necesidad de actualizar las normas de Derecho internacional privado, no solo en materia de Ley aplicable extracontractual, en relación con el Reglamento 864/2007, relativo a la ley aplicable a las obligaciones extracontractuales (Roma II) y el Convenio de la Haya, de 2 de octubre de 1973, sobre Ley aplicable a la Responsabilidad por Productos, que para España tiene primacía sobre el Reglamento, sino también en relación al Reglamento 593/2008, sobre la ley aplicable a las obligaciones contractuales (Roma I).

## 5 Conclusiones

La IA comienza a ser una realidad y, a la vez, un reto para el sistema normativo de cualquier Estado. En la Unión Europea se está trabajando para mitigar las incertidumbres que conlleva y dar confianza. Los métodos tradicionales de regulación no son plenamente aplicables, por lo que debe encontrarse un nuevo planteamiento.

En este contexto, debe prestarse especial atención a todas las cuestiones éticas y legales mencionadas, tan pronto como sea posible, antes de que los problemas relacionados con la inteligencia artificial y su aplicación, incluida la robótica, reciban soluciones parciales y no sistemáticas a nivel nacional.

Esas soluciones parciales dificultarían la colaboración transfronteriza entre Estados, las empresas o la prestación de servicios debido a la necesidad de cumplir diversas normas jurídicas, el aumento del número de controversias comerciales y el incremento de la incertidumbre sobre el rendimiento de las inversiones.

Asimismo, sería necesario analizar y dar respuesta a los problemas de la responsabilidad, la diligencia debida, los contratos sobre sistemas de inteligencia artificial, así como la condición de la inteligencia artificial y la atribución de sus actos de transcendencia jurídica.

## Referencias

ÁLVAREZ RUBIO, J. J. **Difamación y protección de los derechos de la personalidad**: ley aplicable en Europa. Aranzadi: Thomsom Reuters, 2009.

BERTOLINI, A. **Robots and liability**: justifying a change in perspective. Pisa: Pisa University Press, 2014.

BUTTERWORTH, M. The ICO and artificial intelligence: the role of fairness in the GDPR framework. **Computer Law & Security Review**, London, v. 34, n. 2, p. 257-268, abr. 2018.

CALVO CARAVACA, A-L.; CARRASCOSA GONZÁLEZ, J. **Derecho internacional privado.** 18. ed. Granada: Comares, 2018. vol. II.

CARRASCOSA GONZÁLEZ, J. Circulación internacional de datos personales informatizados y la Directiva 95/46/CE. **Actualidad Civil**, Lima, n. 2, p. 509-539, jun. 1997.

COMISIÓN EUROPEA. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. **Inteligencia artificial para Europa** {SWD(2018) 137 final}, COM (2018) 237 final. Bruselas, 25 de abril de 2018. Disponible en: <http://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF>. Consultado el: 20 jun. 2018.

ČERKA, P.; GRIGIENĖ, J.; SIRBIKYTĖ, G. Liability for damages caused by artificial intelligence. **Computer Law & Security Review**, London, v. 31, n. 3, p. 376-389, jun. 2015.

ČERKA, P.; GRIGIENĖ, J.; SIRBIKYTĖ, G. Is it possible to grant legal personality to artificial intelligence software systems? **Computer Law & Security Review**, London, v. 33, n. 5, p. 685-699, oct. 2017.

COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL - CNUDMI/UNCITRAL. **Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales**. Nueva York: CNUDMI, 2007.

COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL - CNUDMI/UNCITRAL. **Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial**: documento presentado por Chequia, Nueva York, 25 de junio a 13 de julio de 2018. Disponible en: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V18/037/81/PDF/V1803781.pdf?OpenElement>. Consultado el: 20 ago. 2018.

CONCLUSIONES del Abogado General, Michal Bobek (2017), presentadas el 13 de julio de 2017, Bolagsupplysningen OÜ, Ingrid Ilsjan contra Svensk Handel AB, asunto C 194/16 (ECLI:EU:C:2017:554). Disponible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=192713&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1884228. Consultado el: 20 maio 2018.

ESLAVA RODRÍGUEZ, M. El locus delicti commissi en los ilícitos contra la vida privada cometidos a través de Internet. **Informática y Derecho**, Mérida, n. 34, p. 13-38, 2002.

FOSCH VILLARONGA, E.; KIESEBERG, P.; LI, T. Humans forget, machines remember: artificial intelligence and the Right to Be Forgotten. **Computer Law & Security Review**, London, v. 34, n. 2, p. 304-313, abr. 2018.

GARAU JUANEDA, L. Las fuentes españolas en materia de ley aplicable a la responsabilidad por ilícito civil. In: JIMÉNEZ PIERNAS, Carlos (Ed.). **La responsabilidad internacional**. Aspectos de Derecho Internacional Público y Derecho Internacional Privado. Alicante: AEPDIRI, 1990. p. 403-450.

GURKAYNAK, G.; YILMAZA, I.; HAKSEVE, G. Stifling artificial intelligence: human perils. **Computer Law & Security Review**, London, v. 32, n. 5, p. 749-758, oct. 2016.

ILLESCAS ORTIZ, Rafael. **Derecho de la contratación electrónica**. Madrid: Civitas, 2011.

LÓPEZ DE MANTARÁS, Ramon. Ética en la inteligencia artificial. **Investigación y ciencia**, Barcelona, n. 491, p. 49, ago. 2017. Disponible en: < https://www.investigacionyciencia.es/files/28484.pdf>. Consultado el: 20 maio 2018.

PALMERINI, E. et al. RoboLaw: Towards a European framework for robotics regulation. **Robotics and autonomous systems**, v. 86, p. 78-85, diciembre 2016. Disponible en: <https://ac.els-cdn.com/S0921889016305437/1-s2.0-S0921889016305437-main.pdf?_tid=514bff82-227c-46a0-a5f8-694c45500fff&acdnat=1543928661_398569569baaeebc0a3b2f659bb9da2f>. Consultado el: 20 maio 2018.

**Recebido em:** 01/10/2018
**Aprovado em:** 05/12/2018