

## *La cultura de la ciberseguridad y la abogacía*

**José Ricardo Pardo Gato**

*Abogado*

### **Resumen**

-

Alcanzar una cultura de ciberseguridad entronca con la necesidad de una ingente labor formativa especializada y generalizada a todos los sectores de la sociedad. Para ello es preciso instaurar una cultura de ciberseguridad acorde y dentro de una más amplia cultura de seguridad y defensa, con afán de implicación de todo el abanico social. En consecuencia, en este ámbito de actuación debe incluirse también, preponderantemente, el sector de la Abogacía.

El secreto profesional y el deber de confidencialidad constituyen elementos fundamentales dentro de los diversos derechos y obligaciones que revisten la exigencia ética del ejercicio diario del abogado. El respeto a estos deberes deontológicos adquiere especial significación ante el desarrollo de los últimos avances tecnológicos y su adecuación a los mismos: inteligencia artificial, *machine learning*, *chatbots*, *bitcoin* y *blockchain*, *big data*...

Algunos de estos avances son ya una realidad, mientras otros, como la robótica, los vemos como algo todavía lejano. En este sentido, prestamos especial atención sobre aquellos que empiezan a estar presentes en las previsiones de la abogacía y la necesidad de la legislación que sobre el tema habrá que articular. El Código Deontológico de la Abogacía Española de 6 de marzo de 2019 es una buena muestra de ello.

**Abstract**

-

*Achieving a culture of cybersecurity is huge specialized and generalized effort for all sectors of society. In order to do this, it is necessary to establish a culture of cybersecurity in accordance with and within a broader culture of security and defense with the involvement of the whole social spectrum. This action should also include the legal profession.*

*Professional secrecy and the duty of confidentiality are key elements within the various rights and obligations that meet the ethical requirement of lawyer's daily practice. Respect for these deontological duties acquires particular significance given the development of the latest technologies and the adaptation to them: artificial intelligence, machine learning, chatbots, bitcoin and blockchain, big data...*

*Some of these advances have already become a reality, while others, such as robotics, still appear as somewhat distant. In this sense, we pay special attention to those which are beginning to be present in the legal profession forecasts and the need for the legislation that will have to be shaped on the subject. The Code of Ethics of the Spanish Legal Profession of March 6, 2019 is a good example of this.*

**Palabras clave:** cultura, abogacía, ciberseguridad, secreto profesional, confidencialidad, inteligencia artificial, machine learning, chatbots, bitcoin, blockchain, big data

**Keywords:** culture, legal profession, cybersecurity, professional secrecy, confidentiality, artificial intelligence, machine learning, chatbots, bitcoin, blockchain, big data

### **Sumario**

- - 1. Desde la aprobación de la “Ley de Internet” hasta los nuevos retos tecnológicos: inteligencia artificial, machine learning, chatbots, bitocin y blockchain, big data...
    - 1.1. La inteligencia artificial
    - 1.2. Machine Learning
    - 1.3. Cibertecnología y deontología
  - 2. El secreto profesional y el deber de confidencialidad adaptados a las ciberseguridad
    - 2.1. Elementos configuradores y definición
    - 2.2. Heterogénea regulación
    - 2.3. Determinación objetiva del secreto profesional: la utilización del sistema LexNET y la Autoridad de Certificación de la Abogacía
  - 3. Conclusiones
    - 3.1. En el ámbito técnico
    - 3.2. En el ámbito normativo
- ANEXO. Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica
- Bibliografía

## I. DESDE LA APROBACIÓN DE LA “LEY DE INTERNET” HASTA LOS NUEVOS RETOS TECNOLÓGICOS: INTELIGENCIA ARTIFICIAL, MACHINE LEARNING, CHATBOTS, BITCOIN Y BLOCKCHAIN, BIG DATA...

La aprobación en el año 2002 de la conocida como “Ley de Internet” [Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI)] puso en el disparadero la vieja polémica existente en la red: un pulso latente entre la libertad de información y el derecho a la intimidad. El temor a los delitos informáticos, el enorme potencial económico de esta malla mundial multimedia y, sobre todo, la diferencia abismal de conocimientos entre simples usuarios y expertos avezados sitúa a estos últimos bajo permanente sospecha<sup>1</sup>.

*Hackers*, *crackers* y *phreakers* son términos que nos vienen a la mente a la hora de poner en solfa la debilidad del sistema informático y el uso de las modernas tecnologías<sup>2</sup>, y más aún aquellos individuos que sobrepasan la frontera de la legalidad y se adentran en el terreno de los conocidos como “delincuentes informáticos”: responsables de robos electrónicos, interceptación de compras online en beneficio propio o falsificación de tarjetas de crédito mediante la duplicidad de las bandas magnéticas, entre otros posibles actos ilícitos.

La aplicación en España tanto de la LSSI como de la posterior legislación sobre firma electrónica [Ley 59/2003, de 19 de diciembre, de firma electrónica

---

<sup>1</sup> Sobre la LSSI y su influencia respecto de la contratación electrónica, en particular la seriada, PARDO GATO, J.R.: *Las páginas web como soporte de condiciones generales contractuales*, Premio Estanislao de Aranzadi 2002, Thomson-Aranzadi, Navarra, 2003; y, para mayor abundamiento, en relación a los delitos informáticos y la ciberseguridad, así como su influencia sobre la ética propia del abogado: *La ciberseguridad como deber deontológico del abogado. El secreto profesional y la protección de datos*, La Ley - Wolters Kluwer, Madrid, 2019.

<sup>2</sup> A los más conocidos “hackers”, se suma también en el argot de la ciberseguridad la palabra “cracker”, aplicable a los expertos que utilizan sus conocimientos para romper contraseñas, entrar en sistemas operativos y causar daño, enriquecerse ilícitamente con esas acciones o propagar virus informáticos; junto con los “phreakers”, aquellas personas que atesoran amplios conocimientos de telefonía y realizan actividades ilegales, como interceptar o hacer llamadas sin que los titulares lo sepan.

(LFE)]<sup>3</sup>, con la implantación del DNI digital y la fiabilidad en la identificación del navegante, supuso sin duda un punto de inflexión en el ámbito de la ciberseguridad en nuestro país, a lo que hay que añadir una tipificación punitiva específica en el Código Penal (CP) para los casos de piratería informática y otros delitos cometidos usando la red<sup>4</sup>.

No obstante, toda esta legislación, aunque ha servido para paliar la ausencia hasta ese momento de una normativa específica al respecto, no ha evitado sin embargo la proliferación de los riesgos informáticos, algunos preexistentes a la fecha de su promulgación y otros nuevos que han ido apareciendo con el tiempo, así como los que ya se intuye formarán parte del futuro más inmediato.

En este contexto, entre estas evoluciones a tener en cuenta, y que se antojan como los retos más importantes a los que hacer frente desde la perspectiva legal, se encuentran:

- La Inteligencia Artificial, con el obligado rediseño de todos los servicios para el móvil.

- La robótica, tomando como ejemplo el conocido robot Ross, considerado el primer abogado “artificialmente inteligente del mundo”, desarrollado desde la Universidad de Toronto y sustentado bajo la plataforma Watson de IBM. Este robot, más bien, lleva a cabo un trabajo específico de un técnico jurídico o de asistente, de servicio “paralegal”, que de un abogado propiamente dicho<sup>5</sup>.

---

<sup>3</sup> Para un comentario respecto de la LFE, me remito al trabajo publicado en PARDO GATO, J.R.: “Encriptación y firma electrónica”, *Internet: un nuevo horizonte para la seguridad y la defensa*, FERNÁNDEZ RODRÍGUEZ, J.J. (ed.), Universidad de Santiago de Compostela, 2010, pp. 185-205.

<sup>4</sup> El espionaje industrial con revelación de secretos obtenidos por medios electrónicos se castiga con la pena de prisión de tres a cinco años (artículo 278 CP). Las estafas cometidas por medios informáticos (artículo 248.2 CP) tienen unas penas de diferente tenor según lo estipulado a su vez en los artículos 249 y 250 CP, que se van endureciendo en función de que concurran determinadas circunstancias que actúan como agravantes. Por su parte, en cuanto a los daños de *hacking maligno* o introducción de virus, se encuentran tipificados en los artículos 264, 264 bis, 264 ter y 264 quater CP.

<sup>5</sup> Desde su aparición en el año 2016, el servicio Ross ha sido contratado por importantes despachos anglosajones, como Carlton Fields o Baker&Hostetler, por poner dos ejemplos. No específicamente ligados al ámbito jurídico, otros robots a los que podemos hacer mención son: el robot Anbot, en China, como robot autónomo, con sensores visuales y acústicos, que constituye un prototipo embrionario para la futura vigilancia y seguridad, así como para la lucha antidisturbios y antiterrorista; el robot Peper, en Japón, capaz de comunicarse e interpretar emociones humanas; el Domino’s Robotic Unit (DRU), en Nueva Zelanda, creado para funciones de reparto de comida rápida; los robots biológicos de Estados Unidos; etc.

- Los asistentes virtuales y el aprendizaje de las máquinas o *machine learning*. A través de algoritmos las personas podrán entrenar a las máquinas y suministrarles un ingente volumen de datos relacionados con sus intereses, de tal manera que estas a su vez los prueban y analizan, establecen coincidencias o diferencias y, en base a todo ello, realizan predicciones en función de unos parámetros determinados. Del mismo modo, están en condiciones de recibir continuamente nuevos datos, así como tomarlos de otras posibles fuentes, con lo que pueden incrementar su capacidad de análisis y predicción.

- Especialmente para la abogacía de persona física, los *chatbots* o robots que charlan, a modo de asistentes virtuales, cuando hablamos por teléfono. Estos robots aproximan el cliente al abogado en todo momento, a través igualmente del análisis predictivo y del aprendizaje automático, con una mejora progresiva en función del mayor número de conversaciones que se lleven a cabo.

- El uso, en el ámbito cambiario general, de criptomonedas o *bitcoin*, así como de los *blockchain* o cadena de bloques, afectará también, ineludiblemente, en el actuar del abogado y en el de otros profesionales, como los registradores. A través de este medio se hace descansar la confianza de los movimientos monetarios en algoritmos matemáticos, y no en las habituales transferencias o transacciones realizadas a través de bancos o entidades similares.

- El big data, término evolutivo que describe cualquier cantidad voluminosa de datos estructurados, semiestructurados y no estructurados que tienen el potencial de ser extraídos para obtener información.

Todas estas novedades que nos brinda el ciberespacio conllevan igualmente un cierto grado de riesgos y amenazas cibernéticas que atenazan la seguridad interna e internacional. Una respuesta eficaz frente a tales peligros no sería posible si no se llega a alcanzar una implicación efectiva de todos los sectores de la sociedad, a través de una cultura de ciberseguridad. Teniendo en cuenta que esta no puede ser atendida individualizada ni aisladamente, sino como parte integrante de una más amplia cultura de seguridad y defensa, se requiere, a los efectos, *“instaurar una cultura de ciberseguridad inserta en una cultura de seguridad y defensa para implicar en ella a toda la sociedad”*<sup>6</sup>.

---

<sup>6</sup> A ello aboga DE TOMÁS MORALES, S.: “Hacia una cultura de ciberseguridad: capacitación especializada para un «proyecto compartido». Especial referencia la ámbito universitario”, *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, núm. 92, mayo-agosto 2014, pp. 13-14.

Algunos de estos avances relacionados son ya una realidad, mientras que otros, como la robótica, los vemos como algo todavía lejano, casi como un desideratum, pero que a buen seguro tendremos que afrontar más pronto que tarde. Me detendré a continuación sobre aquellos que empiezan a estar presentes en las previsiones de los despachos de abogados, por ahora de las grandes firmas, pero que con el tiempo su atención se extenderá a todo el sector de la abogacía; me estoy refiriendo a la inteligencia artificial y al *machine learning*.

### **1.1. La inteligencia artificial**

La inteligencia artificial (IA), también llamada “inteligencia computacional”, es, de entre todas las novedades tecnológicas referidas, la que plantea a priori mayores esfuerzos de adaptación por parte de la Abogacía, ora institucional, ora individual o de ejercicio colectivo. Ha sido considerada, de hecho, como el fenómeno sobre el que se sustentará la denominada “cuarta revolución industrial”, que será objeto de estudio para las futuras generaciones como uno de los hitos más grandes de la humanidad, con un impacto tal como el que tuvo en su día el fuego o la electricidad<sup>7</sup>. Se trata, ni más ni menos, que de la inteligencia exhibida por las máquinas: término empleado para referirse a cualquier tipo de software capaz de ejecutar una tarea o función normalmente asociada a una persona, por requerir de una cierta inteligencia o capacidad intuitiva.

Así, en el ejercicio profesional la IA puede servir de base al abogado en diversos ámbitos de actuación<sup>8</sup>:

- *Localización y revisión de contratos y documentos*: este instrumento resulta idóneo para la búsqueda de documentación y contratos, a través de la localización de términos, expresiones o frases que se relacionan o encajan con un determinado criterio predefinido. Es un modo de robotizar la gestión de la documentación legal gracias al procesamiento del lenguaje natural. De esta manera, se facilita a los abogados y a otros profesionales jurídicos poder manejar

---

<sup>7</sup> Así lo afirmó recientemente la CEO de Google, Sunder Pichai, traída a colación en el artículo del coorganizador del primer Congreso sobre *Legaltech* en España, en 2017, MORELL RAMOS, J.: “La Inteligencia Artificial en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará”, *Abogacía Española*, núm. 108, febrero 2018, pp. 7 y 8.

<sup>8</sup> A ellas se refirió también BRUCH MASERAS, E.: “I.A.: qué es, cuál usar y cómo”, *Abogacía Española*, núm. 108, febrero 2018, p. 9.

en mejores condiciones, y de una manera más sencilla, la información que precisan, tanto para la preparación de litigios como para procedimientos *due diligence*.

En este sentido, es importante para la comparación de documentación contractual por medio de la detección de cláusulas coincidentes o no coincidentes, adicionales o inexistentes, así como el grado de divergencia que puede haber entre las mismas; clasificación de las estipulaciones y de los propios contratos conforme el tipo de que se trate, fechas, importes que en ellos aparezcan, etc.; o como variación de valores económicos objeto de pacto según estadios predeterminados de precios o garantías. Desde un punto de vista práctico, una vez fijado un criterio, por ejemplo “Localiza todos los contratos firmados por el despacho en los últimos 3 años”, la IA encuentra esa información específica y sobre ella se puede establecer una serie de reglas o parámetros que faciliten a la postre el trabajo del abogado.

- *Búsqueda de información, doctrina, legislación y jurisprudencia*: hablamos no solo de un simple tecleo de una frase o palabra clave en un buscador de internet, sino de un barrido más inteligente, tecnológica o “artificialmente” hablando, así como de una búsqueda más rápida y eficaz, teniendo en cuenta de manera primordial el contexto que engloba o rodea determinados términos, que es precisamente lo que concreta y separa la información relevante de la no pertinente.

- *Analítica predictiva*: fundamentada en un análisis predictivo de resultados para el planteamiento de diferentes estrategias de actuación. Tras analizar el ingente volumen de precedentes con los que cuenta, la IA se convierte en un medio o herramienta idónea cuando de predecir resultados judiciales se refiere o de estimación de probabilidades de que el juzgador falle en un sentido u otro a tenor del histórico profesional del juez en cuestión. Y lo mismo cabría decir, por ejemplo, cuando queremos estimar el importe de una indemnización por despido o por accidente de circulación, o el de una pensión alimenticia que el letrado pretenda solicitar para su cliente. Pero es en el ámbito de búsqueda jurisprudencial donde la IA presenta mayores ventajas al letrado, dado que, como afirma BRUCH MASERAS, “*la analítica es capaz de detectar los argumentos con los que un juez tradicionalmente falla en positivo o en negativo*”<sup>9</sup>, lo que redundará en una valiosa información para el abogado a la hora de preparar sus escritos de demanda o

---

<sup>9</sup> Cfr. “I.A.: qué es...”, cit., p. 9.



contestación, así como también poder calcular el tiempo estimado en el que el juez o el tribunal dictará sentencia según la sala conocedora del asunto.

- *Preliminares en la preparación de una demanda o escrito de contestación:* partiendo, por tanto, de la analítica predictiva y de la propia búsqueda avanzada e inteligente referida, el abogado podrá disponer de la información requerida para el desarrollo de un primer borrador de demanda o contestación, en base precisamente a los algoritmos lógicos que actúen sobre la documentación con la que cuenta la IA, así como de las tendencias de emisión de sentencias de aquellos jueces sobre los que recaerá el deber de juzgar el caso concreto.

- *Sistemas automatizados de diagnóstico encaminados a aportar solución a determinadas situaciones jurídicas:* en consonancia a todo lo anterior, la IA también posibilita la creación de sistemas automatizados de diagnóstico, con la pretensión de resolver específicos problemas jurídicos que se planteen. Y ello, en base al recurso a soluciones web ejecutables a demanda de los abogados o usuarios, configurables de acuerdo a la información y/o documentación que estos incorporen, y que a su vez será debidamente contrastada por la aplicación. Todo lo cual se traducirá en la sugerencia de posibles soluciones a la situación propuesta o la emisión de ciertos diagnósticos a temas suscitados.

## 1.2. Machine learning

Una rama de la inteligencia artificial aplicada (conocida como *Weak AI*) es el *machine learning*, sistema con el que se pretende conseguir que las máquinas aprendan de una forma automática.

Como apuntamos, se trata de un modelo de aprendizaje automático fundamentado en el entrenamiento de algoritmos, con el objetivo de que, “*a partir de patrones obtenidos del análisis de datos, realicen predicciones perfeccionando modelos que nos ayuden a generar ideas y tomar mejores decisiones*”<sup>10</sup>. En este sentido, para un aprendizaje mayor, que dotará a la máquina a su vez de un mejor funcionamiento, cobra importancia el volumen de datos e información con la que cuente, así como del algoritmo de que se trate, ya sean algoritmos supervisados por humanos [tanto

---

<sup>10</sup> MOLINA PÉREZ-TOMÉ, S.: “*Machine Learning* en el sector legal”, *Abogacía Española*, núm. 108, febrero 2018, p. 14.

para la entrada (inputs) como para la salida de datos (outputs)] o no supervisados (*deep learning*).

En la actualidad, el *machine learning* ha entrado de lleno en el sector de la abogacía, y de los profesionales del Derecho en general, a través de diversos proyectos de *Legaltech*, basados en el uso de la tecnología y el software en servicios de tipo legal: software de gestión, generación de contratos, documentos legales y reclamaciones online, marketing digital jurídico, etc. Sin duda, con este sistema se puede contribuir a un notable ahorro de costes y de tiempo, así como de proyección de trabajos, favoreciendo la consiguiente transformación digital de los despachos.

### **1.3. Cibertecnología y deontología**

Toda esta modernidad y avances tecnológicos, con sus potencialidades y beneficios, junto con los problemas de adaptación que toda novedad supone, habrán de casar igualmente con los tradicionales postulados éticos, de sentir humano y de calado profesional, entre los que se encuentran los deberes deontológicos que desde antiguo le asisten al abogado.

Y así como para perseguir la piratería informática nació una nueva policía, el “ciberdetective”, como cuerpos de seguridad especializados en seguir los pasos de una actividad tecnológica ilícita desde el PC atacado hasta el ordenador o máquina de la que partió la intromisión, pasando necesariamente por el prestador de servicios<sup>11</sup>, también en el ámbito deontológico el abogado habrá de valerse de los servicios técnicos y jurídicos que la nueva realidad digital y cibertecnológica le ofrecen para garantizar su buen proceder profesional. Igual adaptación deberán realizar asimismo los colegios de abogados, como vigías que son del debido cumplimiento ético por parte de sus colegiados, entre otros aspectos: el deber de secreto profesional y la confidencialidad que debe prevalecer entre este y su cliente.

---

<sup>11</sup> En España, tanto la Guardia Civil, con su Grupo de Delitos de Alta Tecnología, como la Policía Nacional, por medio de la Brigada de Investigación Tecnológica (BIT), vigila el ciberespacio a la búsqueda de delincuentes informáticos. En este sentido, el Grupo de Delitos de Alta Tecnología de la Guardia Civil se encuentra integrado por personal debidamente seleccionado y sus miembros cuentan con conocimientos avanzados de informática, telecomunicaciones e idiomas, a través de varios cursos de formación en universidades y centros especializados; además, está íntimamente relacionado con otros grupos policiales especializados en la investigación de delitos informáticos de todo el mundo, como el FBI (EE.UU), New Scotland Yard (Reino Unido), Gendarmería Nacional (Francia), Bundeskriminalamt (Alemania), Policía Montada (Canadá) o NPA (Japón), entre otros.

A este respecto, existe ya un Proyecto de Informe de la Comisión de Asuntos Jurídicos del Parlamento Europeo con recomendaciones destinadas a la Comisión relativa a las normas de Derecho civil sobre robótica [2015/2103 (INL)], publicado el 31 de mayo de 2016, en lo que constituye el primer texto europeo sobre esta cuestión y el principal referente a tener en cuenta en relación a dicha materia<sup>12</sup>. En este informe se detalla una propuesta de resolución en la que, entre otras cuestiones, se incluye: la obligatoriedad de un seguro de responsabilidad civil específico; establecer un fondo de compensación; un régimen de responsabilidad limitada para el fabricante, el programador, el propietario o el usuario (un fondo general para todos los robots autónomos inteligentes o un fondo individual para cada categoría de robots); la creación de un número de inscripción individual que ha de figurar en un registro específico europeo; y, dando un paso más, la configuración de una personalidad jurídica propia para los robots.

Pero, por lo que a nuestro estudio afecta, lo más relevante del referido informe del Parlamento Europeo es que para dar soporte ético a todas estas propuestas, por ejemplo en cuanto a la intimidad, la integridad, la autonomía y la protección de datos, se considera preciso un marco deontológico que sirva de orientación sobre todos estos aspectos. Así, se propone, como anexo a la resolución del informe, una carta sobre robótica, un código de conducta ética para los ingenieros de robótica y un código deontológico para los comités de ética de la investigación. Textos pioneros en Europa sobre normativa ética en el uso de la robótica y la inteligencia artificial, antesala de una futura regulación comunitaria centrada en su utilización, que han de ser tenidos muy en cuenta también a los efectos de la ética predicable en el actuar del abogado cuando intervengan tales medios.

Y es que la confianza imprescindible que ha de existir a la hora de contratar los servicios de un abogado, e igualmente a lo largo del desarrollo de su labor de asesoramiento y defensa jurídica, no es algo que la inteligencia artificial y los nuevos desarrollos tecnológicos puedan reemplazar fácilmente. No obstante, la confianza debe seguir siendo el pilar principal sobre el que se sostiene la calidad del trabajo letrado y los esfuerzos de la abogacía habrán de ir encaminados a su preservación y puesta permanente en valor. Por ello, el secreto profesional y el

---

<sup>12</sup> Este informe puede consultarse en la web del Parlamento Europeo: <https://www.europarl.europa.eu>.

deber de confidencialidad habrán de mantenerse inalterables como postulados básicos de la profesión, cuya preservación debe estar siempre garantizada con independencia de los procedimientos de los que podamos servirnos en cada momento.

## **2. EL SECRETO PROFESIONAL Y EL DEBER DE CONFIDENCIALIDAD ADAPTADOS A LA CIBERSEGURIDAD**

Pese a ser un deber deontológico inherente a la condición de abogado, aún en el siglo XXI el secreto profesional constituye uno de los aspectos más controvertidos a los que se enfrenta la práctica de una abogacía moderna y renovada. No en vano se trata de un auténtico derecho/deber, cuyo reconocimiento legal y deontológico no puede ser cuestionado por nadie, pero cuya interrelación genera numerosas fricciones, pues en ocasiones no es fácil delimitar con rotundidad sus límites y contenidos<sup>13</sup>.

Y no puede ser de otro modo, ya que nos adentramos en un terreno en el que deben congeniar la apreciación y el criterio subjetivo del abogado, en su faceta de profesional, con el respeto a algunos de los derechos que en el ordenamiento jurídico alcanzan el estatus de fundamentales, tales como el derecho a la intimidad y el derecho de defensa que asiste a todo ciudadano, potencial cliente.

Cohonestar estos aspectos primordiales con la seguridad requerida y con la ciberseguridad, en cuanto a los elementos tecnológicos se refiere, resulta de obligada atención y cumplimiento para el adecuado desarrollo de la abogacía en su adaptación ineludible a los nuevos tiempos. Máxime cuando estos novedosos elementos adquieren carta de naturaleza si lo que se quiere garantizar es la mayor de las seguridades en el ejercicio de la profesión.

Dentro de este marco de actuación, la propia IA, como la hemos definido, podría indicarle al software que los contratos consistentes en NDAs, o acuerdos de confidencialidad, sean directamente dirigidos o enviados a una persona concreta, por ejemplo al propio cliente, y este destinatario sepa fehacientemente quien se los envía, en este caso su abogado. Esta es solo una de las posibilidades que se abren a

---

<sup>13</sup> En cuanto a la delimitación del secreto profesional del abogado, vid. PARDO GATO, J.R.: *La relación abogado-cliente. El contrato de servicios del abogado*, Premio Memorial Degà Roda i Ventura del Colegio de Abogados de Barcelona, Colección Grandes Tratados, Aranzadi, Navarra, 2017, pp. 187-215.

la hora de poner estos nuevos medios tecnológicos al servicio de la ética profesional del abogado.

En todo caso, la obligada adaptación a las novedades que la evolución de la sociedad impone no debe alejarnos un ápice de los tradicionales requisitos deontológicos que marcan el devenir profesional del letrado, partiendo para ello de sus elementos configuradores.

### **2.1. Elementos configuradores y definición**

El abogado hace las veces de depositario de los secretos que guarda su cliente, que a la vez considera que los deja a buen recaudo, y es asimismo destinatario, primero y último, de las comunicaciones confidenciales, electrónicas o no, que se realizan entre ambos<sup>14</sup>. Por ello, el Código de Deontología de los Abogados de la Unión Europea valora el secreto profesional como el derecho, pero también la obligación, fundamental y primordial del abogado (artículos 2.3 y 3.2)<sup>15</sup>.

Para poder llevar a cabo la mejor de las defensas el letrado precisa conocer toda la información relevante y necesaria que atesora su cliente, cuya confianza e intimidad debe quedar totalmente salvaguardada por el secreto profesional que a ambos incumbe. Como declara el preámbulo del actual Código Deontológico de la Abogacía Española (CD), aprobado por el Pleno del Consejo General de la Abogacía Española el 6 de marzo de 2019 (con entrada en vigor el 8 de mayo de 2019), “[e]l ciudadano precisa asesoría jurídica –requiere, por tanto, de la figura del abogado– para conocer el alcance y trascendencia de sus actos, y, para ello, debe confesarle sus circunstancias más íntimas”, hasta el punto de que el menor de los detalles puede resultar el dato central que favorezca el mejor asesoramiento y defensa

---

<sup>14</sup> Estos son dos de los elementos que remarcan el carácter singular de la profesión de abogado, como se resaltó en PARDO GATO, J.R.: *La singularidad de la Abogacía (De entre las profesiones liberales)*, Premio Jurídico Internacional del Instituto Superior de Derecho y Economía (ISDE), Difusión Jurídica-Economist&Jurist, Madrid, 2017. Como señala SÁNCHEZ STEWART, N., en el prólogo a dicha obra: “El autor enmarca la singularidad que proclama para la Abogacía en la peculiar y muy reforzada exigencia al proceder intachable de quienes la ejercen, que deben observar este respecto irrestricto a las normas de contenido ético y social que conforman la deontología. Reglas de actuación –sigue diciendo Nielson– que al ser aprobadas por órganos competentes, los institucionales de la Abogacía desde tiempo inmemorial, como reconoce el Tribunal Constitucional español, se transforman en normas jurídicas de obligado cumplimiento, so pena de aplicación de sanciones disciplinarias”.

<sup>15</sup> Como derecho o privilegio, vid. INTERNATIONAL BAR ASSOCIATION: *Privilege and confidentiality*, Londres, 2006.

jurídica. En este sentido, resulta primordial que todos estos datos y confidencias se mantengan a buen recaudo, con independencia del medio que empleen abogado y cliente para comunicarse, ya sea tecnológico o no.

Pero mientras la generalidad de la doctrina considera que el origen del secreto profesional es ético y no contractual<sup>16</sup>, y su naturaleza no es absoluta sino relativa<sup>17</sup>, su bien jurídico protegido, en el ámbito de las personas físicas, es la inmunidad personal<sup>18</sup>, o bien la confianza<sup>19</sup>; y en el de las personas jurídicas, la competencia leal o capacidad competitiva de la empresa<sup>20</sup>.

Por lo demás, puede decirse que el secreto profesional del abogado no es un concepto unívoco en todo el mundo<sup>21</sup>, pues existen diferencias entre la definición tradicional acogida por el Derecho continental europeo y la particular del Derecho anglosajón<sup>22</sup>. Y ello pese a que ambos sistemas jurídicos tienen como común

---

<sup>16</sup> DEL ROSAL, R.: *Normas deontológicas de la Abogacía Española. Una doctrina construida a partir del ejercicio de la competencia disciplinaria*, Civitas, Madrid, 2002, p. 88.

<sup>17</sup> RIGO VALLBONA, J.: *El secreto profesional de abogados y procuradores en España*, Bosch, Barcelona, 1988, p. 104.

<sup>18</sup> MUÑOZ CONDE, F.: *Derecho Penal. Parte especial*, 12ª ed., Tirant lo Blanch, Valencia, 1999, p. 252, que considera que la intimidad, como bien jurídico protegido del secreto profesional (artículo 199 CP), se deriva del derecho a la defensa.

<sup>19</sup> CORTÉS BECHIARELLI, E.: *El secreto profesional del abogado y el procurador y su proyección penal*, Marcial Pons, Madrid, 1998, pp. 56-94, para quien el bien jurídico *primario* protegido por el artículo 199.2 CP es la confianza.

<sup>20</sup> MUÑOZ CONDE, F.: *Derecho Penal...*, *ob. cit.*, p. 479, que estima que el bien jurídico protegido en el ámbito de las empresas se encuentra recogido en los artículos 278 y ss. CP.

<sup>21</sup> MULLERAT BALMAÑA, R.M.: "Confidente o cancerbero (algunas consideraciones sobre el secreto profesional del abogado)", *La Ley*, núm. 5783, de 19 de mayo de 2003, para quien "el secreto profesional del Abogado no es un concepto único y sólido en todo el mundo. En la tradición del Derecho romanístico civil (*Civil Law*), el secreto profesional es único, absoluto, con poquísimas excepciones y sancionado penalmente. En cambio, en la tradición del *Common Law* se distingue entre la «confidencialidad» (*confidentiality*), que es un deber ético, y el «privilegio Abogado-cliente» (*attorney-client privilege*), que es una norma de Derecho probatorio que exime al Abogado de dar testimonio en los procesos judiciales respecto de la información que recibe de su cliente. Por otro lado, para la tradición del Derecho civil, el secreto pertenece al orden público y el Abogado no puede, como he adelantado, revelarlo ni con la autorización del cliente. En cambio, para la del *Common Law*, el secreto se considera pertenece al Cliente y, por tanto, el propio Cliente puede relevar al Abogado de la obligación de guardar secreto".

<sup>22</sup> Como sostiene ÁLVAREZ-SALA WALTHER, J.: *El blanqueo de capitales y las profesiones jurídicas*, Ensayos de actualidad de escritura pública, Consejo General del Notariado, Madrid, 2004, pp. 12 y ss.: "la circunstancia de ser ese privilegio accesorio a la confidencialidad y estar ésta, como relación contractual privada, sometida a la ley, determina que el secreto profesional tenga en la práctica jurídica angloamericana una significación menos intensa y explica leyes tan polémicas como la Patriot Act del año 2001, excluyendo la confidencialidad entre los detenidos por terrorismo y sus abogados, o la Oaxley-Sarbanes Act del año 2002, dictada tras el caso ENRON, que obliga a los abogados a denunciar cualquier infracción de la normativa en

denominador la idea fundamental, ya en origen, de que el secreto profesional es la pieza esencial en la relación abogado-cliente<sup>23</sup>.

En España, por su parte, si el *Diccionario de la Lengua*, en su segunda acepción, hace referencia expresa a la “reserva” y al “sigilo”<sup>24</sup>, se ha venido proponiendo por algún autor una definición, bastante más completa, que compartimos en términos generales: “*El deber de secreto profesional es una obligación de orden e interés público que, con fundamento moral y social, nace como consecuencia de un conocimiento adquirido por una persona, en razón o con motivo del ejercicio por la misma de una profesión cuya existencia y desempeño son necesarios a los miembros de la sociedad en un determinado estado de cultura, en virtud de la cual obligación el profesional no puede comunicar a otros aquel conocimiento*”<sup>25</sup>.

## 2.2. Heterogénea regulación

Así conceptualizado, el secreto profesional ha sido considerado -e incluso delimitado-, principalmente, a través de una serie de reglas de deontología y ética profesional, en gran medida relativas al abogado. Pero su regulación también encuentra cabida, en general, en el Derecho positivo, en el que, transversalmente y de un modo un tanto parcial, se hace mención al mismo en un buen número de postulados que perfilan este principio básico: normas de tenor constitucional<sup>26</sup>,

---

*materia de valores. Igualmente Gran Bretaña tiene también leyes en materia de terrorismo y blanqueo de capitales (la Anti-Terrorist, Crime and Security Act y la Money Laundering Regulation, ambas del 2001) que imponen a los Abogados deberes de denuncia”.*

<sup>23</sup> Así, ZURITA CARRIÓN, J.: “El secreto profesional: razón y límites”, *Deontología y práctica de la Abogacía del siglo XXI*, Aranzadi, Navarra, 2008, p. 52. También MULLERAT BALMAÑÁ, R.M.: “Confidente o cancerbero...”, cit., considera “*que en ambas tradiciones la confianza y su secuela, el secreto profesional, constituyen el epicentro de la relación cliente-abogado*”, a lo que añade que “*Abogados y Colegios tienen este principio en gran estima y todos los códigos de deontología del mundo reconocen su importancia y protegen su cumplimiento*”.

<sup>24</sup> REAL ACADEMIA ESPAÑOLA: *Diccionario de la Lengua Española*, 22<sup>a</sup> ed., Madrid, 2001, p. 2036, que en su primera acepción lo identifica con la “[c]osa que cuidadosamente se tiene reservada y oculta”, y en la tercera con el “[c]onocimiento que exclusivamente alguien posee de la virtud o propiedades de una cosa o un procedimiento útil en medicina o en otra ciencia, arte u oficio”.

<sup>25</sup> Definición aportada por RIGO VALLBONA, J.: *El secreto profesional de abogados y procuradores en España*, Bosch, Barcelona, 1998, p. 79.

<sup>26</sup> La Ley Orgánica del Poder Judicial (LOPJ), en su artículo 542.3, dispone que los abogados “deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos”.

civil<sup>27</sup>, penal<sup>28</sup>, laboral<sup>29</sup>, procesal<sup>30</sup>, y hasta de orden tributario<sup>31</sup>, hacen mención expresa, directa o indirectamente, al mismo, lo que nos indica su enorme importancia de cara al buen hacer en el ejercicio de la profesión.

Sin embargo, es dentro de la normativa deontológica donde el secreto profesional encuentra, en puridad, su razón de ser. En primer término, cabría referirse al vigente Estatuto General de la Abogacía Española del año 2001 (EGAE/2001), aprobado por Real Decreto 658/2001, de 22 de junio [en concreto, sus artículos 25.2.a), 32, 34.e) y 42.1; correlativos a su vez en la redacción prevista en el Estatuto General aprobado el 12 de junio de 2013 por unanimidad del Consejo General de la Abogacía Española (EGAE/2013), pendiente de ratificación legislativa: artículos 21.2.a), 25, 23 y 11.1]. También en este ámbito deberemos tener en cuenta el actual Código Deontológico de la Abogacía Española [en particular, sus artículos 5, 6.2 y 6.3.a, 11.2 y 11.11, 12.A.5, 12.B.2.j, así como el párrafo final del artículo 12.B.2, 12.B.3 –en cuanto a la referencia sobre protección de datos de

---

<sup>27</sup> Ley Orgánica 1/1982, de 5 de mayo, de protección civil al honor, a la intimidad y a la propia imagen.

<sup>28</sup> El artículo 199 del Código Penal castiga al “que revelase secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales” y al “profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona”. Asimismo, los artículos 278 a 280 de este mismo código regulan el denominado “secreto industrial o empresarial”. Por su parte, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, mantiene la inclusión de los abogados entre los sujetos que vienen obligados a colaborar con la respectiva unidad financiera en la prevención del blanqueo de dinero.

<sup>29</sup> Dado que el secreto se extiende por parte de los sujetos obligados a los empleados, dependientes y colaboradores del abogado, el Real Decreto 1331/2006, de 17 de noviembre, por el que se regula la relación laboral de carácter especial de los abogados que prestan servicios en despachos de abogados, individuales o colectivos, desarrolla esta obligación para los sujetos que dependen del titular del despacho, como así se establece en los artículos 6 y 24.2 en lo relativo a la responsabilidad disciplinaria.

<sup>30</sup> En el ámbito procesal civil, el artículo 371 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, referente a los testigos con deber de guardar secreto. Y, en el ámbito procesal penal, el artículo 263 de la Ley de Enjuiciamiento Criminal dispone que la obligación de denuncia “no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieron de sus clientes”, mientras que el artículo 416.2 dispensa de la obligación de declarar al abogado del procesado en lo referente “a los hechos que éste le hubiere confiado en su calidad de defensor”.

<sup>31</sup> Incluso la Administración tributaria ha de respetar, en todo momento, el secreto profesional del abogado, como así se infiere del matiz que el artículo 93.5 de la Ley 58/2003, de 17 de diciembre, General Tributaria, realiza respecto del principio general de colaboración que ha de existir con la misma.



carácter personal-, 12.C.4 y 21.2, que deben complementarse, a su vez, con los artículos 2.3 y 3.2 del Código Deontológico de los Abogados de la Unión Europea].

Es en el contexto de la anterior regulación donde el secreto profesional encuentra su fundamento, que no es otro que la necesidad de proteger a las personas del perjuicio que le podría ocasionar la revelación de secretos confiados necesariamente a otro ciudadano en razón de su profesión y en cuyo silencio confían.

Si la existencia del profesional es lo que garantiza la relación de confidencialidad con el cliente, algo esencial en toda prestación de servicio, cuando hablamos de prestación jurídica la misma se fundamenta en ese carácter personal (*intuitio personae*), intelectual e independiente. Así lo ha venido a declarar el Tribunal Supremo, que en su sentencia de 17 de febrero de 1998 (RJ 1998, 1633) declaró que el secreto profesional era el fundamento del derecho de defensa y, en otra de fecha 3 de marzo de 2003 (RJ 2003, 2643), llegó a calificarlo como la “*piedra angular de la Abogacía*”, sobre la que bascula.

### **2.3. Determinación objetiva del secreto profesional: la utilización del sistema LexNET y la Autoridad de Certificación de la Abogacía**

Al igual que establecen los artículos 542.3 LOPJ y 32.1 EGAE/2001 (artículo 22 EGAE/2013), el Código Deontológico, en su artículo 5.1, indica, con carácter general, que el abogado tiene el derecho y deber, simultáneamente, de guardar secreto profesional “respecto de los hechos o noticias que conozca por razón de cualquiera de las modalidades de su actuación profesional” (proclamación que, en el ámbito europeo, sigue también el Código Deontológico del CCBE en su artículo 2.3.1). El abogado recibe o conoce de muy diversas confidencias, documentos y hechos, pero a diferencia de otros profesionales que también están obligados al sigilo (médicos, periodistas, investigadores, etc.), el letrado ha de actuar como filtro de ese conocimiento, es decir, decide conforme a su mejor criterio cuáles de aquellos hechos o confidencias han de ser utilizadas en el ejercicio de la defensa de los derechos del cliente.

Por tanto, el secreto profesional incluye las comunicaciones con clientes, con compañeros o con el adversario, y comprende “todos los hechos y documentos de que haya tenido noticia o haya remitido o recibido por razón de cualquiera de

las modalidades de su actuación profesional” (artículo 5.2 CD). Extensión que aparecía más detallada en el artículo 5.3 del anterior Código Deontológico del año 2002, al referirse también “a las cartas, comunicaciones o notas que reciba del abogado de la otra parte”; así como en el nuevo texto del Estatuto General de 2013, al delimitarla ampliamente respecto de “todos los hechos, comunicaciones, datos, informaciones, documentos y propuestas que, como Abogado, haya conocido, emitido o recibido en su ejercicio profesional” (artículo 23.1 EGAE/2013)<sup>32</sup>.

Por otra parte, el abogado debe guardar sigilo de todas aquellas noticias, hechos o documentos que han podido llegar a su conocimiento o a su poder por cualquier medio o circunstancia -por tanto, también a través de medios tecnológicos-, y cualquiera que sea la forma que revista su ejercicio profesional, ya sea mero asesoramiento o gestión jurídica, o bien defensa letrada en los tribunales. En este sentido, el Tribunal Supremo, en su sentencia de 16 de diciembre de 2003 (RJ 2005, 3604), confirma que abarca incluso los hechos públicos o notorios; y en la de 22 de abril de 1997 (RJ 2007, 3094), le vale para definir el marco en el que se mueve la reserva y la confidencialidad, al incluir los borradores y las meras conversaciones orales, sin que se exija la firma -electrónica o no- en los documentos, por lo que entendemos que dicho secreto se extendería al propio contrato, verbal o escrito, que el abogado haya pactado con su cliente.

La normativa deontológica hace referencia igualmente a las conversaciones presenciales y a distancia, tanto con el cliente como con la parte contraria -ha de suponerse, en presencia del cliente y de su abogado-, así como también con los abogados de la otra parte. Pero esta afirmación no significa que puedan quedar excluidas de secreto profesional aquellas conversaciones que, de la misma forma, pudiera mantener el abogado con personas que sin tener la condición de clientes, contrarios o abogados, se relacionen, de un modo u otro, con el letrado dentro de su ámbito profesional, ya sea un familiar del cliente, un investigador privado, un perito, un testigo, etc.

---

<sup>32</sup> No obstante, si la preservación, en cualquier caso, de la reserva sobre las confidencias y propuestas de los compañeros, aun con la oposición del cliente al mantenimiento del secreto, debe resultar deontológicamente adecuada, no parece razonable, sin embargo, otorgar idéntico tratamiento al adversario, salvo cuando se hayan conocido sus informaciones a través de su letrado [STS, Sala Tercera, Sección Sexta, de 10 de mayo de 1999 (RJ 1999, 4799)].

Cuando nos referimos a conversaciones a distancia, siguiendo para ello lo establecido en el Código Deontológico, el Estatuto General de 2013 hace ya mención expresa a los medios electrónicos y contempla la posible existencia de grabaciones. Así, al traer a colación las conversaciones mantenidas por los abogados con sus clientes, los contrarios o sus abogados, ambos textos indican que las mismas pueden ser “de presencia o por cualquier medio telefónico o telemático”<sup>35</sup>, a lo que añaden -en términos explícitos en este caso del Estatuto General, si bien muy similares a los del Código Deontológico- que “solo podrán ser grabadas con la previa advertencia y conformidad de todos los intervinientes,

---

<sup>35</sup> En cuanto al medio telefónico, el Tribunal Supremo ha ratificado que el secreto profesional ampara las comunicaciones del abogado con su cliente, por ejemplo en la STS, Sala Primera, de 25 de abril de 2002, en la que condena a un magistrado por intervenir las conversaciones telefónicas mantenidas entre clientes, presos a la sazón, y sus abogados. Si bien la STS, Sala Segunda, de 28 de noviembre de 2001 (RJ 2001, 10328), afirma que “*el secreto profesional que protege las relaciones de abogados con sus clientes puede, en circunstancias excepcionales, ser interferido por decisiones judiciales que acuerden la intervención telefónica de los aparatos instalados en sus despachos profesionales. Es evidente que la medida reviste una incuestionable gravedad y tiene que ser ponderada cuidadosamente por el órgano judicial que la acuerda, debiendo limitarse a aquellos supuestos en que existe una constancia, suficientemente contrastada, de que el abogado ha podido desbordar sus obligaciones y responsabilidades profesionales integrándose en la actividad delictiva, como uno de sus elementos componentes*”. Respecto a tribunales menores, vid. ATSJ Madrid, Sala de lo Civil y Penal, 28/2010, de 25 de marzo de 2010 (JUR 2010, 101019), que resuelve los recursos de apelación interpuestos contra el AAN del Juzgado Central de Instrucción núm. 5 y contra el AJI de Madrid de 27 de enero de 2010.

Por su parte, el Tribunal Europeo de Derechos Humanos (TEDH), en su sentencia de 13 de marzo de 2007 (*caso Castravet contra Moldavia*), advirtió que “*una injerencia en el privilegio abogado cliente, y por ende, en el derecho del detenido a la defensa, no exige necesariamente que tenga lugar una interceptación real o una escucha subrepticia. Una creencia genuina, basada en indicios razonables de que su conversación está siendo escuchada, puede ser suficiente, desde el punto de vista del Tribunal, para limitar la efectividad de la asistencia que el abogado pueda proporcionar*”. Mientras que en la STEDH de 25 de marzo de 1998 (*caso Kopp contra Suiza*), el mismo tribunal ya había señalado que la injerencia existe desde la interceptación de las comunicaciones, sin que sea relevante la posterior utilización de las grabaciones; y en la STEDH de 2 de agosto de 1984 (*caso Malone*) que el secreto de las comunicaciones, y en especial de las postales, telegráficas y telefónicas, se extiende tanto al conocimiento del contenido de las mismas, como a la identidad de los interlocutores [así, también, SSTEDH de 6 de junio de 1978 (*caso Klass*), 12 de junio de 1988 (*caso Schenk*) y los dos fallos de 24 de abril de 1993 (*casos Kruslin y Huvig*)]. En cuanto a que, en relación también a las escuchas telefónicas, debe existir una proporción entre la intromisión de esta clase de prueba y la finalidad perseguida, el TEDH asienta dicha afirmación en la satisfacción de una necesidad imperiosa y proporcionada a la finalidad perseguida [SSTEDH de 7 de diciembre de 1976 (*caso Handsyde*), 26 de abril de 1979 (*caso The Sunday Times*), 24 de marzo de 1988 (*caso Olsson*) y 21 de junio de 1988 (*caso Berrehab*)].

Sobre los medios telefónicos, vid. CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA: “La intervención de las comunicaciones del imputado con su abogado quien, a su vez, es decano de un colegio”, Informe 3/2015, Comisión Jurídica del CGAE, 28 de julio de 2015. Por su parte, en relación a los medios telemáticos, téngase en cuenta la regulación contenida en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y de Comercio Electrónico.

quedando en todo caso amparadas por el secreto profesional” (artículos 5.4 CD y 23.3 EGAE/2013). No obstante, la redacción del Estatuto General de 2013 va más allá, cuando puntualiza que quedan además bajo secreto profesional “las grabaciones realizadas por el cliente, no conocidas por su Abogado, incluso si éste no lo era o no intervino en dicho momento, de conversaciones en que intervenga el Abogado de la otra parte”. Autorizadas o no, todas estas grabaciones no podrán ser utilizadas o aportadas en juicio, salvo que medie el consentimiento expreso de todos los intervinientes en las conversaciones de que se trate.

Hay que tener en cuenta, como se ha alertado, que el uso de las tecnologías de la información pone en peligro el secreto profesional de nuevos modos y maneras poco conocidas hasta hace no demasiado tiempo y que, en cualquier caso, obligan al abogado a estar precavido ante los nuevos retos. Un ejemplo, muy concreto y plenamente extendido, lo constituye el uso por los profesionales, además del resto de ciudadanos, del correo electrónico y las comunicaciones vía internet, bien con el propio cliente, bien con el compañero que se encarga de la representación del contrario, e incluso con los tribunales, por ejemplo a través de la plataforma LexNET.

De hecho, partiendo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que refunde parte de la anterior Ley 30/1992 y de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, a modo de proyección del procedimiento administrativo electrónico (procedimiento obligatorio para los abogados, entre otros profesionales que precisen de colegiación obligatoria para ejercer su actividad), la aprobación de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, y la posterior entrada en vigor del Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET, profundizan en dicha exigibilidad en las comunicaciones de los abogados y procuradores con esta Administración pública<sup>34</sup>.

---

<sup>34</sup> Para mayor abundamiento sobre el sistema LexNET, téngase en cuenta la página web [https://www.administraciondejusticia.gob.es/paj/publico/ciudadano/informacio\\_institucional/modernizacion\\_tecnologica/infolexnet](https://www.administraciondejusticia.gob.es/paj/publico/ciudadano/informacio_institucional/modernizacion_tecnologica/infolexnet).

Este sistema, denominado LexNET, se configura así como una plataforma de intercambio seguro de información entre los órganos judiciales y una gran diversidad de operadores jurídicos que, en su trabajo diario, necesitan intercambiar documentos judiciales, en particular notificaciones, escritos, demandas y contestaciones. Tras años de adaptación (este modelo electrónico empezó a funcionar en el año 2004, siendo obligatorio desde el 1 de enero de 2016), podemos decir que LexNET se ha convertido en un trabajo seguro tan habitual en el ámbito de las comunicaciones judiciales como el teléfono, el fax o el correo electrónico.

A este respecto, también desde la implantación de la Autoridad de Certificación de la Abogacía (ACA) por parte del Consejo General de la Abogacía Española<sup>35</sup>, los certificados digitales emitidos por esta autoridad certificadora son certificados reconocidos según la meritada Ley de Firma Electrónica. Además de identificar al titular que lo ostenta, garantizan su condición de abogado, lo cual le permite ejercer profesionalmente a través de internet con plena validez jurídica. De este modo, el carnet colegial no solo facilita la identificación física al abogado que lo aporte, sino que el chip que contiene incorpora a su vez el dispositivo seguro de creación de la firma electrónica correspondiente.

Desde un punto de vista práctico, la utilización del carnet colegial posibilita de esta manera poder realizar un buen número de gestiones vía online, tanto para el servicio de los propios usuarios, los abogados, como cuando se lleva a cabo en representación de los clientes: procedimientos de jura de cuentas; tramitación de pases a prisión; solicitar y obtener certificados de la Seguridad Social; declaración, liquidación y pago de impuestos; entre otros.

Desde la perspectiva organizativa, la condición profesional queda acreditada, en último término, por los colegios de abogados que, en su calidad de autoridades de registro, son los responsables de la emisión, suspensión y revocación de los certificados digitales<sup>36</sup>.

---

<sup>35</sup> Consúltese la web <https://www.acabogacia.org/acabogacia/home.do>.

<sup>36</sup> Sobre el tema, vid. AA.VV.: *E-Abogacía*, CREMADES, J. (coord. jurídico) y BADÍA Y LIBERAL, E. (coord. periodístico), La Ley, Madrid, 2007; PARDO GATO, J.R.: “La abogacía ante el desarrollo de las nuevas tecnologías, en el libro del VIII Congreso de la Abogacía Española. Libro de ponencias y comunicaciones, Consejo General de la Abogacía Española, Aranzadi, Navarra, 1999, pp. 322-332; “La defensa letrada y el devenir tecnológico”, *Foro Galego*, revista del Ilustre Colegio de Abogados de A Coruña,

Por otro lado, la obligación de guardar el secreto profesional por parte del abogado permanece incluso después de haber cesado en la prestación de los servicios al cliente o abandonado el despacho donde se estaba incorporado, a lo que el artículo 5.8 del Código Deontológico se cuida en aclarar “sin que esté limitada en el tiempo”. Así, bajo esta redacción, la citada norma no sujeta dicha obligación a límite temporal alguno, con lo que se prolongaría a lo largo de la existencia del abogado, incluso después de haber cesado en su ejercicio profesional, y con independencia de que pudiera producirse su baja colegial. Esta misma característica de intemporalidad no deja de afectarle aunque hubiese devenido el fallecimiento del cliente, pues su muerte no extinguiría el deber de secreto que le asiste al abogado.

En consecuencia, todos los datos, informaciones y documentos que el abogado reciba de su cliente, tanto durante la prestación del servicio jurídico como posteriormente a haber desarrollado su labor, deben quedar perfectamente salvaguardados dentro del secreto profesional que a aquel le asiste. Todos estos datos, que abarcan, como no podía ser de otro modo, los de carácter personal, no deben, por ende, ser objeto de análisis, ni antes ni después, por parte de la inteligencia artificial ni de sus sucedáneos tecnológicos, lo que conllevaría una flagrante infracción de dicho deber de sigilo.

### **3. CONCLUSIONES**

#### **3.1. En el ámbito técnico**

Como se ha podido comprobar, de un tiempo a esta parte es en el ámbito de la ciberseguridad donde la obligación profesional letrada de preservar la confidencialidad en la relación abogado-cliente adquiere una nueva dimensión, de tal forma que el empleo cada vez más generalizado de la tecnología y los procedimientos de protección apropiados se convierten en una necesidad deontológica.

Afirmaciones como la de que *“la inteligencia artificial y la revolución de las máquinas se encuentran entre las ocho tecnologías disruptivas que cambiarán el mundo y por*

---

de la Real Academia Gallega de Jurisprudencia y Legislación, y de la Universidad de A Coruña, núms. 196-197, segundo semestre 2006-primer semestre 2007, pp. 337-374; y, en particular en relación a la firma digital, “Encriptación y firma electrónica”, *Internet: un nuevo horizonte para la seguridad y la defensa*, FERNÁNDEZ RODRÍGUEZ, J.J. (ed.), Universidad de Santiago de Compostela, 2010, pp. 185-205.

*extensión nuestra sociedad*<sup>37</sup>, describen el sentir actual. Pero su empleo debe llevarse a cabo manteniendo la debida confidencialidad y bajo la permanente protección del secreto profesional. En caso contrario podríamos estar poniendo en peligro la seguridad de un sistema susceptible de resultar vulnerable, así como de toda la información alojada en aquel, lo que derivaría en un incumplimiento del deber deontológico aplicable ante una eventual infracción de dicho secreto<sup>38</sup>.

Para evitar estos efectos, ya a principios del siglo XXI se contemplaban determinadas medidas técnicas de seguridad en aras a evitar ataques de virus en la red, que podrían resultar igualmente aplicables en la actualidad; a saber: no abrir ningún mensaje de correo electrónico de un remitente desconocido, pues la mayoría de virus llegan por email; descarga de programas y aplicaciones solo de sitios seguros de la red, ya que los que se ofrecen gratuitamente pueden estar infectados; no ejecutar archivos descargados del email sin pasarlos antes por un antivirus; no facilitar la dirección de correo electrónico a cualquiera, con lo que se evitaran los *spammers* y posibles virus; cambiar la contraseña del correo electrónico con regularidad; etc.

También la Abogacía española reaccionó a estos peligros con la creación de la Autoridad Certificadora de la Abogacía. La utilización por parte de los colegiados de la firma electrónica ACA garantiza la seguridad jurídica y técnica de las comunicaciones que realicen, y les proporciona un entorno de seguridad que les protege frente a posibles ataques informáticos o suplantaciones de identidad que pueden poner en riesgo el secreto profesional al que todos los abogados vienen obligados.

Esta autoridad certificadora establece igualmente un decálogo con recomendaciones a seguir en cuanto al tratamiento de la protección de datos<sup>39</sup>: los datos personales son siempre de su titular, no de quien los maneja; afecten o no a la intimidad, deben de tratarse con pleno respeto a la legislación aplicable y las medidas de seguridad; siempre ha de respetarse el deber de confidencialidad de los datos; estos deben utilizarse solo para la finalidad para la que fueron recabados; no

---

<sup>37</sup> GUARDIOLA SALMERÓN, M.: "Retos, desafíos y nuevas oportunidades", *Abogacía Española*, núm. 108, febrero 2018, p. 10.

<sup>38</sup> Vid. <https://www.abogacia.es/2017/05/25/la-ciberseguridad-en-la-deontologia-del-abogado>.

<sup>39</sup> <https://www.abogacia.es/2018/05/10/protección-de-datos-para-abogados>.

deben dejarse datos a la vista de terceros, debiendo aplicarse una política de mesas limpias; se ha de evitar extraer datos personales fuera del lugar de trabajo, y si resultara imprescindible, deben utilizarse dispositivos con medidas de seguridad; cuando se manejen datos, habrán de emplearse siempre servicios de correo electrónico o de almacenamiento que respeten la legislación aplicable; no debe dejarse nunca abierto el ordenador propio, sin que tampoco las claves de acceso queden a la vista; y no pueden tirarse documentos con datos personales a las papeleras, sino que han de utilizarse los destructores de papel.

Junto con las precedentes medidas, que podríamos calificar de tradicionales, con la irrupción de la inteligencia artificial y el resto de novedades tecnológicas las instituciones y organizaciones implicadas vienen compelidas a facilitar a los interesados información y medios de cómo actuar en cada caso. Un ejemplo a seguir es la *Guía sobre cómo gestionar una fuga de información en un despacho de abogados*, publicada en el año 2016 por la Agencia Española de Protección de Datos (AEPD), en colaboración con el propio Consejo General de la Abogacía Española y el Instituto Nacional de Ciberseguridad (INCIBE)<sup>40</sup>.

Es justamente desde ese mismo año cuando, en el marco de actuación de la *redabogacía*, el Consejo General de la Abogacía ha dado pasos firmes en la transición de la antigua plataforma del *correo de la Abogacía* a *Office 365*, con el fin de dotar a los colegiados con herramientas que le permitan tener su despacho a un clic y en la nube<sup>41</sup>.

Ahondando en lo anterior, se pretende, entre otras soluciones: la migración de la infraestructura tecnológica del Consejo a la nube, en lo que vendría a ser la *nube de la Abogacía*, y que posibilitará gestionar de forma más eficiente y segura el

---

<sup>40</sup> Esta guía puede consultarse en la dirección de internet: [https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/INCIBE\\_AEPD\\_Gestionar\\_fuga\\_de\\_informacion.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/INCIBE_AEPD_Gestionar_fuga_de_informacion.pdf).

<sup>41</sup> PÉREZ ANDÚJAR, C.: "REDABOGACÍA: impulsando y liderando la transformación tecnológica de la Abogacía española", *Abogacía Española*, núm. 108, febrero 2018, p. 29, señala que el potencial que tiene la herramienta del *correo Abogacía* sitúa al colectivo letrado a la vanguardia de los colectivos profesionales: "Disponemos de un buzón de correo de 50 Gb, 1 TB de almacenamiento en la nube (OneDrive), gestión profesional de agendas, contactos, tareas, soporte técnico al usuario. Podemos trabajar online con nuestros documentos de Microsoft Office (Word, Excel, PowerPoint) sin necesidad de tenerlo instalado, guardarlos de forma segura en la nube, compartir ficheros con clientes, otros miembros del despacho, el Colegio. Y mucho más (mensajería instantánea, videoconferencias, reuniones en internet, etc.)".



almacenamiento de los datos con los que cuentan los abogados; la implantación del *expediente digital*, habida cuenta de que tanto el Consejo como los colegios de abogados han de adaptar sus procesos de trabajo y sus sistemas para poder cumplir debidamente con lo que dispone la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en cuanto a la obligación que incumbe a tales corporaciones de comunicarse telemáticamente con la Administración; o la transformación del *Sistema Integral de Gestión de la Abogacía* (SIGA: herramienta que protege la información de los colegios usuarios al encontrarse alojada en el centro de datos de la Infraestructura Tecnológica de la Abogacía Española), hacia un nuevo modelo más moderno, funcional e intuitivo, con el objetivo de facilitar los trámites a seguir entre consejo, colegios y colegiados.

En cuanto a este último avance, al estar en la nube de la Abogacía, el personal del colegio autorizado accede a SIGA desde cualquier terminal u ordenador y en cualquier momento, lo que contribuye a hacer más eficiente el trabajo diario. En este sentido, SIGA está interconectado con las Administraciones públicas, y esa interconexión permite al Consejo General de la Abogacía, según la propia consejera y vicesecretaria de medios materiales y tecnológicos del Consejo, Carmen PÉREZ ANDÚJAR, “*estar a la vanguardia en eJusticia ofreciendo servicios únicos que conectan los Colegios con las Comisiones de Asistencia Jurídica Gratuita, la Agencia Tributaria, la Seguridad Social y otros Organismos*”<sup>42</sup>. Mediante este sistema integral de gestión toda la información se encuentra protegida bajo estrictas medidas de seguridad físicas y lógicas, conforme a los requisitos exigidos por la Ley Orgánica de Protección de Datos.

Pero, además de SIGA, concedores de que desde hace tiempo cualquier sistema informático puede verse afectado por un incidente de ciberseguridad, el mismo Consejo General ha venido desarrollando acciones de concienciación, formación y sensibilización entre los abogados<sup>43</sup>. En todas estas actuaciones se insiste en la obligación del letrado de mantener la debida protección de los datos que gestiona y la seguridad de los sistemas que los albergan: efectuando, por ejemplo, constantes acciones de mantenimiento, actualización y pruebas de resiliencia, incluyendo auditorías de seguridad periódicas<sup>44</sup>. Y, del mismo modo,

---

<sup>42</sup> Et. al., p. 30.

<sup>43</sup> <https://www.abogacia.es/tag/ciberseguridad>.

<sup>44</sup> <https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos>.

cómo esa exigencia compele a la inclusión de estas necesidades de seguridad dentro de la gestión de riesgos cibernéticos que puedan afectar, de un modo u otro, a la información de los clientes<sup>45</sup>.

Sin perjuicio de lo anterior, y dado que la tecnología nunca es del todo segura, los abogados deberemos exigir asimismo a nuestros proveedores tecnológicos externos que sus productos cumplan diligentemente con las obligaciones de seguridad que imponen las normas legales y deontológicas aplicables<sup>46</sup>.

Con independencia de esta última medida, siempre nos queda desear, a nivel técnico, que los nuevos avances tecnológicos vayan de la mano de la aparición de novedosos medios o instrumentos de ciberseguridad que nos permitan a su vez, acompasadamente, dotar de mecanismos de protección y salvaguarda de la documentación y de los datos personales aportados por los clientes. Todo ello redundará, sin duda, en el cumplimiento de los deberes deontológicos que exige el ejercicio de la abogacía.

### **3.2. En el ámbito normativo**

Si en la funcionalidad técnica reside una importante necesidad de implementación de las medidas a adoptar para responder a la constante modernización tecnológica, las estrategias de seguridad acogidas por los Estados modernos constituyen un instrumento idóneo para la generalización de una cultura de la ciberseguridad en las respectivas sociedades avanzadas. Para ello, se requiere de un eficaz desarrollo legislativo y un auténtico compromiso por parte de los distintos gobiernos, administraciones y organismos públicos implicados en que su arraigo sea una realidad. En este sentido, comparto la afirmación de TOMÁS MORALES de que *“los responsables de diseñar un plan de actuación –acción unitaria- frente a las ciberamenazas, no deberían olvidar la necesidad de insertarlo dentro del marco de una cultura de la seguridad y la defensa nacional, interna e internacional”*<sup>47</sup>.

---

<sup>45</sup> <https://www.abogacia.es/2012/03/14/guias-tic-gestion-de-riesgos>.

<sup>46</sup> Así lo asevera PÉREZ BES, F.: “Lo que nos enseñan las crisis de ciberseguridad”, *Abogacía Española*, núm. 109, mayo 2018, p. 29.

<sup>47</sup> DE TOMÁS MORALES, S.: “Hacia una cultura de ciberseguridad...”, cit., p. 43.

Llevado al terreno de la abogacía, y a sabiendas de que el ordenamiento jurídico no deja de ser más que un reflejo de la constante y permanente evolución y transformación de la sociedad en que vivimos, esta profesión debe saber adaptarse a esta nueva realidad sin perder su esencia y sus valores éticos más tradicionales, como es el secreto profesional y la obligación de confidencialidad.

La robótica y la inteligencia artificial, el machine learning, los bitcoins y blockchain, chatbots o big data, junto a otras tecnologías (como las impresoras 3D, la computación, la realidad virtual y aumentada, los vehículos autónomos o la biotecnología), han ido cambiando nuestra percepción de entender el mundo. Por extensión, y como no puede ser de otra manera, esta transformación ha de ir ligada, indisolublemente, al modo de comprender el Derecho y la forma de ejercer las profesiones jurídicas, aunque no podamos sostener por el momento que Ross pueda sustituir hoy por hoy a un abogado. Para contratar los servicios letrados es imprescindible la confianza, y eso no es algo que la IA pueda reemplazar fácilmente, a resultas de que ese valor es intrínseco a la calidad del servicio jurídico: sin confianza no puede establecerse la relación abogado-cliente.

El primero, y por ahora único, paso legislativo dado en esta materia ha sido en 2016 a través del citado Proyecto europeo relativo a las normas de Derecho civil sobre robótica, que incide también, eso sí desde un prisma diferente, en los aspectos éticos a tener en cuenta. No obstante, todavía es prematuro hablar de legislación en un ámbito de actuación ni mucho menos consolidado. Pero, teniendo presente la vertiginosa rapidez con la que este sector está avanzando, no resulta descabellado anticipar debates jurídicos que a buen seguro abrirán nuevos retos desde el punto de vista legal y que, consecuentemente, nos harán reconfigurar nuestra manera convencional de entender el Derecho<sup>48</sup>.

Es evidente que todavía nos queda mucho por andar en este iniciado recorrido de la IA y de los nuevos avances tecnológicos descritos. No en vano, la realidad viene anticipando lo que no desde hace mucho considerábamos mera ficción, debido precisamente a la latente ebullición del desarrollo científico y tecnológico, creciente y en ascenso, que vivimos en los últimos tiempos en la sociedad.

---

<sup>48</sup> Así lo entiende también GUARDIOLA SALMERÓN, M.: "Retos, desafíos...", cit., p. 12.

Algo que solo era mera ilusión en nuestra imaginación, ha pasado de un estado de gestación inicial a convertirse en una constatación cada vez más palpable, y cuya evolución augura un resultado mayor de lo inicialmente esperado. Todo ello supondrá, sin duda, un cambio en la concepción de nuestro día a día y, por ende, de la forma de entender el ordenamiento jurídico. Esto llevará, a su vez, a la abogacía a replantear la concepción clásica del Derecho y su aplicación práctica, sin menoscabar en ningún momento el respeto a los parámetros éticos y deontológicos exigibles, entre ellos, preponderantemente, el secreto profesional y la debida confidencialidad.

## ANEXO

### INFORME

27.I.2017

PE 582.443v02-00 A8-0005/2017

**con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica**  
[2015/2103(INL)]

Comisión de Asuntos Jurídicos

Ponente: Mady Delvaux

(Iniciativa – artículo 46 del Reglamento)

Ponentes de opinión (\*):

Georg Mayer, Comisión de Transportes y Turismo

Michał Boni, Comisión de Libertades Civiles, Justicia y Asuntos de Interior

(\* ) Procedimiento de comisiones asociadas – artículo 54 del Reglamento

### PROPUESTA DE RESOLUCIÓN

#### DEL PARLAMENTO EUROPEO

**con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica**

*El Parlamento Europeo,*

– Visto el artículo 225 del Tratado de Funcionamiento de la Unión Europea,

- Vista la Directiva 85/374/CEE sobre la responsabilidad por los daños causados por productos defectuosos,
- Vistos los artículos 46 y 52 de su Reglamento,
- Vistos el informe de la Comisión de Asuntos Jurídicos y las opiniones de la Comisión de Transportes y Turismo, de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de la Comisión de Empleo y Asuntos Sociales, de la Comisión de Medio Ambiente, Salud Pública y Seguridad Alimentaria, de la Comisión de Industria, Investigación y Energía, y de la Comisión de Mercado Interior y Protección del Consumidor (A8-0005/2017),

### **Introducción**

- A. Considerando que, desde el monstruo de Frankenstein creado por Mary Shelley al mito clásico de Pígalión, pasando por el Golem de Praga o el robot de Karel Čapek —que fue quien acuñó el término—, los seres humanos han fantaseado siempre con la posibilidad de construir máquinas inteligentes, sobre todo andróides con características humanas;
- B. Considerando que, ahora que la humanidad se encuentra a las puertas de una era en la que robots, bots, andróides y otras formas de inteligencia artificial cada vez más sofisticadas parecen dispuestas a desencadenar una nueva revolución industrial —que probablemente afecte a todos los estratos de la sociedad—, resulta de vital importancia que el legislador pondere las consecuencias jurídicas y éticas, sin obstaculizar con ello la innovación;
- C. Considerando que es necesario crear una definición generalmente aceptada de robot y de inteligencia artificial que sea flexible y no lastre la innovación;
- D. Considerando que, entre 2010 y 2014, las ventas de robots aumentaron un 17 % de media cada año, que en 2014 las ventas registraron el mayor incremento anual observado hasta ahora —a saber, un 29 %—, y que los principales motores de este crecimiento son los proveedores de componentes de automoción y la industria electrónica y eléctrica; que a lo largo del último decenio se han triplicado las solicitudes anuales de patentes en el sector de la tecnología robótica;

- E. Considerando que durante los últimos doscientos años las cifras de empleo han aumentado de manera continuada gracias al desarrollo tecnológico; que el desarrollo de la robótica y de la inteligencia artificial tiene potencial para transformar el modo de vida y las formas de trabajo, aumentar los niveles de eficiencia, ahorro y seguridad y mejorar la calidad de los servicios, y que se espera que, a corto y medio plazo, la robótica y la inteligencia artificial traigan consigo eficiencia y ahorro, no solo en la producción y el comercio, sino también en ámbitos como el transporte, la asistencia sanitaria, las operaciones de salvamento, la educación y la agricultura, permitiendo que los seres humanos dejen de exponerse a condiciones peligrosas, como, por ejemplo, las que entraña la limpieza de lugares contaminados con sustancias tóxicas;
- F. Considerando que el envejecimiento de la población se debe al aumento de la esperanza de vida propiciado por los avances en las condiciones de vida y en la medicina moderna, y que se trata de uno de los principales retos políticos, sociales y económicos a los que se enfrentan las sociedades europeas del siglo XXI; que en 2025 más de un 20 % de los europeos habrá cumplido los sesenta y cinco años, con un aumento especialmente rápido de la población mayor de ochenta años, lo que dará lugar a un equilibrio radicalmente diferente entre las generaciones dentro de nuestra sociedad, y que redundará en beneficio de la sociedad y de las familias que las personas de edad avanzada se mantengan saludables y activas el mayor tiempo posible;
- G. Considerando que, a largo plazo, la tendencia actual que apunta al desarrollo de máquinas inteligentes y autónomas, con capacidad de ser entrenadas para pensar y tomar decisiones de manera independiente, no solo implica ventajas económicas, sino también distintas preocupaciones relativas a sus efectos directos e indirectos en el conjunto de la sociedad;
- H. Considerando que el aprendizaje automático ofrece enormes ventajas económicas e innovadoras a la sociedad, al mejorar enormemente la capacidad de analizar datos, aunque también plantea retos a la hora de velar por la no discriminación, las garantías procesales, la transparencia y la inteligibilidad de los procesos decisorios;

- I. Considerando que, de modo similar, es necesario evaluar los cambios económicos y los efectos en el empleo ocasionados por la robótica y el aprendizaje automático; que, a pesar de las innegables ventajas de la robótica, su utilización puede entrañar una transformación del mercado de trabajo y la necesidad de reflexionar en consecuencia sobre el futuro de la educación, el empleo y las políticas sociales;
- J. Considerando que, si bien es posible que el uso generalizado de robots no acarree automáticamente la sustitución de puestos de trabajo, sí que es probable que los empleos menos cualificados en sectores intensivos en mano de obra sean más vulnerables a la automatización; que esta tendencia podría devolver procesos de producción a la Unión; que la investigación ha demostrado que el crecimiento del empleo es considerablemente más rápido en los puestos de trabajo que hacen un mayor uso de la informática; que la automatización de los puestos de trabajo puede liberar a las personas de tareas manuales monótonas y permitirles que se dediquen a otras más creativas y significativas; que la automatización obliga a los Gobiernos a invertir en educación y a acometer otras reformas con el fin de mejorar la redistribución en los tipos de capacidades que necesitarán los trabajadores en el futuro;
- K. Considerando que, al mismo tiempo, el desarrollo de la robótica y la inteligencia artificial puede dar lugar a que los robots asuman gran parte del trabajo que ahora realizan los seres humanos sin que puedan reemplazarse por completo los empleos perdidos, cuestión esta que genera interrogantes sobre el futuro del empleo y la viabilidad de los sistemas de seguridad y bienestar sociales y sobre la insuficiencia continuada de las cotizaciones para los regímenes de jubilación, en caso de que se mantenga la actual base imponible, lo que podría acarrear una mayor desigualdad en la distribución de la riqueza y el poder, mientras que, en el marco de la financiación del apoyo y reciclaje profesional para desempleados cuyos puestos de trabajo se hayan reducido o eliminado, deberá estudiarse la posibilidad de someter a impuesto el trabajo ejecutado por robots o exigir un gravamen por el uso y mantenimiento de cada robot, a fin de mantener la cohesión social y la prosperidad;



- L. Considerando que, a la vista de las crecientes fracturas sociales y el declive de la clase media, conviene tener en cuenta que el progreso de la robótica podría traducirse en una elevada concentración de la riqueza y el poder en manos de una minoría;
- M. Considerando que no cabe duda de que el desarrollo de la robótica y la inteligencia artificial incidirá en el panorama del empleo, lo que puede crear nuevas preocupaciones relativas a la responsabilidad y eliminar otras; que debe aclararse la responsabilidad jurídica desde el punto de vista del modelo de empresa y de la definición de las tareas de los trabajadores, en caso de que se produzca una emergencia o surjan problemas;
- N. Considerando que la tendencia hacia la automatización requiere que los implicados en el desarrollo y comercialización de aplicaciones de inteligencia artificial incorporen desde el principio características de seguridad y ética, reconociendo de ese modo que deben estar preparados para aceptar la responsabilidad jurídica respecto de la calidad de la tecnología que producen;
- O. Considerando que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (1) (Reglamento general de protección de datos) establece un marco jurídico para la protección de los datos personales; que puede resultar necesario abordar otros aspectos relativos al acceso de los datos y a la protección de los datos personales y la intimidad, habida cuenta de las preocupaciones que en esta materia aún podrían suscitar las aplicaciones y los dispositivos que se comunican entre sí y con bases de datos sin intervención humana;
- P. Considerando que la evolución en la robótica y en la inteligencia artificial puede y debe concebirse de modo que preserve la dignidad, la autonomía y la autodeterminación del individuo, especialmente en el ámbito de la atención y la compañía a las personas, y en el contexto de los dispositivos médicos que «reparen» o mejoren a los seres humanos;
- Q. Considerando que existe la posibilidad de que a largo plazo la inteligencia artificial llegue a superar la capacidad intelectual humana;

- R. Considerando que el desarrollo de toma de decisiones automatizadas y basadas en algoritmos y su creciente utilización incidirán sin duda en las elecciones de los particulares (por ejemplo, empresas o usuarios de internet) y de las autoridades administrativas y judiciales u organismos públicos de otro tipo, a la hora de tomar su decisión final, ya sea de carácter comercial, de ejercicio de la autoridad pública o de consumo; considerando que es necesario integrar salvaguardias y la posibilidad de control y verificación por parte de las personas en los procesos de toma de decisiones automatizados y basados en algoritmos;
- S. Considerando que en varios países extranjeros, como los EE.UU., Japón, China y Corea del Sur, se están planteando adoptar medidas normativas en el ámbito de la robótica y la inteligencia artificial, y que en algunos casos ya han empezado a hacerlo; que algunos Estados miembros han empezado también a reflexionar sobre la posible elaboración de normas jurídicas o la introducción de cambios legislativos a fin de tener en cuenta las nuevas aplicaciones de dichas tecnologías;
- T. Considerando que la industria europea podría resultar beneficiada de un enfoque normativo adecuado, eficiente, transparente y coherente a escala de la Unión que defina unas condiciones previsibles y lo suficientemente claras para que las empresas puedan desarrollar aplicaciones y planificar sus modelos de negocio a escala europea, garantizando al mismo tiempo que la Unión y sus Estados miembros conservan el control sobre la normativa que se haya de establecer, de modo que no se vean obligados a adoptar o aceptar normas establecidas por otros, es decir, por terceros países que también están a la vanguardia del desarrollo de la robótica y la inteligencia artificial;

### **Principios generales**

- U. Considerando que debe entenderse que las leyes de Asimov (2) van dirigidas a los diseñadores, fabricantes y operadores de robots, incluidos los que disponen de autonomía y capacidad de autoaprendizaje integradas, dado que dichas leyes no pueden traducirse en código máquina;

- V. Considerando que es necesario disponer de una serie de normas en materia de responsabilidad, transparencia y rendición de cuentas que reflejen los valores humanistas intrínsecamente europeos y universales que caracterizan la contribución de Europa a la sociedad; que esas normas no deben afectar al proceso de investigación, innovación y desarrollo en el ámbito de la robótica;
- W. Considerando que la Unión podría desempeñar un papel esencial a la hora de establecer principios éticos básicos que deban respetarse en el desarrollo, la programación y la utilización de robots y de la inteligencia artificial, y a la hora de incorporar dichos principios a la normativa y los códigos de conducta de la Unión, con el fin de encauzar la revolución tecnológica para que esté al servicio de la humanidad y, de este modo, los beneficios de la robótica y la inteligencia artificial más avanzadas se distribuyan de la manera más amplia, evitando, dentro de lo que cabe, posibles escollos;
- X. Considerando que en las futuras iniciativas en materia de robótica e inteligencia artificial, la Unión debe adoptar una actitud gradual, pragmática y prudente, como la propugnada por Jean Monnet (3), a fin de asegurarse que no se ponen trabas a la innovación;
- Y. Considerando que, dado el nivel de desarrollo alcanzado por la robótica y la inteligencia artificial, procede empezar por las cuestiones relativas a la responsabilidad civil;

### **Responsabilidad**

- Z. Considerando que, gracias a los impresionantes avances tecnológicos de la última década, los robots ya no solo pueden realizar actividades que antes eran típica y exclusivamente humanas, sino que el desarrollo de determinados rasgos cognitivos y autónomos —como la capacidad de aprender de la experiencia y tomar decisiones cuasi independientes— ha hecho que estos robots se asimilen cada vez más a agentes que interactúan con su entorno y pueden modificarlo de forma significativa; que, en este

contexto, es crucial la cuestión de la responsabilidad jurídica por los daños que pueda ocasionar la actuación de los robots;

- AA. Considerando que la autonomía de un robot puede definirse como la capacidad de tomar decisiones y aplicarlas en el mundo exterior, con independencia de todo control o influencia externos; que esa autonomía es puramente tecnológica y que será mayor cuanto mayor sea el grado de sofisticación con que se haya diseñado el robot para interactuar con su entorno;
- AB. Considerando que, cuanto más autónomos sean los robots, más difícil será considerarlos simples instrumentos en manos de otros agentes (como el fabricante, el operador, el propietario, el usuario, etc.); que esta circunstancia, a su vez, suscita la cuestión de si la normativa general sobre responsabilidad es suficiente o si se requieren normas y principios específicos que aporten claridad sobre la responsabilidad jurídica de los distintos agentes y su responsabilidad por los actos y omisiones de los robots cuya causa no pueda atribuirse a un agente humano concreto, y de si los actos u omisiones de los robots que han causado daños podrían haberse evitado;
- AC. Considerando que, en última instancia, la autonomía de los robots suscita la cuestión de su naturaleza y de si pertenecen a una de las categorías jurídicas existentes o si debe crearse una nueva categoría con sus propias características jurídicas;
- AD. Considerando que, en el actual marco jurídico, los robots no pueden ser considerados responsables de los actos u omisiones que causan daños a terceros; que las normas vigentes en materia de responsabilidad contemplan los casos en los que es posible atribuir la acción u omisión del robot a un agente humano concreto —como el fabricante, el operador, el propietario o el usuario—, y en los que dicho agente podía haber previsto y evitado el comportamiento del robot que ocasionó los daños; que, además, los fabricantes, los operadores, los propietarios o los usuarios podrían ser considerados objetivamente responsables de los actos u omisiones de un robot;

- AE. Considerando que, según el marco jurídico vigente, la responsabilidad por daños causados por productos defectuosos —en la que el fabricante de un producto es responsable de un mal funcionamiento— y las normas que rigen la responsabilidad por una actuación que ocasiona daños —en la que el usuario de un producto es responsable de un comportamiento que deriva en un perjuicio— se aplican a los daños ocasionados por los robots o la inteligencia artificial;
- AF. Considerando que, en el supuesto de que un robot pueda tomar decisiones autónomas, las normas tradicionales no bastarán para generar responsabilidad jurídica por los daños ocasionados por el robot, ya que no permitirán determinar la parte que ha de hacerse cargo de la indemnización, ni exigir a dicha parte que repare el daño ocasionado;
- AG. Considerando que también son manifiestas las deficiencias del marco jurídico vigente en el ámbito de la responsabilidad contractual, ya que la existencia de máquinas concebidas para elegir a sus contrapartes, negociar cláusulas contractuales, celebrar contratos y decidir sobre su aplicación hace inaplicables las normas tradicionales, lo que pone de relieve la necesidad de adoptar nuevas normas eficientes y actualizadas, acordes con los avances tecnológicos y las innovaciones recientemente aparecidas y utilizadas en el mercado;
- AH. Considerando que en materia de responsabilidad extracontractual podría no ser suficiente el marco ofrecido por la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985 (4), que solo cubre los daños ocasionados por los defectos de fabricación de un robot a condición de que el perjudicado pueda demostrar el daño real, el defecto del producto y la relación de causa a efecto entre el defecto y el daño (responsabilidad objetiva o responsabilidad sin culpa);
- AI. Considerando que, pese al ámbito de aplicación de la Directiva 85/374/CEE, el marco jurídico vigente no bastaría para cubrir los daños causados por la nueva generación de robots, en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento, ya que un robot podría aprender

de forma autónoma de sus experiencias concretas e interactuar con su entorno de un modo imprevisible y propio únicamente a ese robot;

### **Principios generales relativos al desarrollo de la robótica y la inteligencia artificial para uso civil**

1. Pide a la Comisión que proponga definiciones europeas comunes de sistema ciberfísico, sistema autónomo, robot autónomo inteligente y sus distintas subcategorías, tomando en consideración las siguientes características de un robot inteligente:
  - capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el intercambio y análisis de dichos datos;
  - capacidad de autoaprendizaje a partir de la experiencia y la interacción (criterio facultativo);
  - un soporte físico mínimo;
  - capacidad de adaptar su comportamiento y acciones al entorno;
  - inexistencia de vida en sentido biológico;
2. Considera que debe crearse un sistema global de registro de robots avanzados dentro del mercado interior de la Unión en los casos en que sea pertinente y necesario para subcategorías específicas de robots, y pide a la Comisión que establezca criterios para la clasificación de los robots que tendrían que registrarse; pide a la Comisión, en este contexto, que analice la conveniencia de que la gestión del sistema de registro y de las inscripciones se atribuya a una agencia de la Unión para la robótica y la inteligencia artificial;
3. Pone de relieve que el desarrollo de la tecnología robótica debe orientarse a complementar las capacidades humanas y no a sustituirlas; considera fundamental garantizar que, en el desarrollo de la robótica y los sistemas de inteligencia artificial, los seres humanos tengan en todo momento el control sobre las máquinas inteligentes; estima que debe prestarse especial

atención al posible desarrollo de un vínculo emocional entre seres humanos y robots —especialmente en el caso de grupos vulnerables, como niños, personas mayores y personas con discapacidad—, y destaca los problemas que pueden plantear las graves consecuencias físicas y emocionales que este vínculo emocional podría causar a los seres humanos;

4. Subraya que un enfoque a escala de la Unión puede facilitar el desarrollo, evitando la fragmentación del mercado interior, y pone de relieve, al mismo tiempo, la importancia del principio de reconocimiento mutuo en el uso transfronterizo de robots y sistemas robóticos; recuerda que la realización de ensayos, la certificación y la autorización de comercialización deberían exigirse solo en un Estado miembro; destaca que este enfoque debería complementarse con una vigilancia de mercado eficaz;
5. Subraya la importancia de tomar medidas de apoyo a las pequeñas y medianas empresas y a las empresas emergentes del sector de la robótica que creen nuevos segmentos de mercado en este ámbito o que utilicen robots en sus actividades;

### **Investigación e innovación**

6. Subraya que muchas aplicaciones robóticas están todavía en fase experimental; se congratula de que cada vez sea mayor el número de proyectos de investigación financiados por los Estados miembros y la Unión; considera esencial que la Unión, junto con los Estados miembros a través de la financiación pública, siga estando en la vanguardia de la investigación en robótica e inteligencia artificial; pide a la Comisión y a los Estados miembros que refuercen los instrumentos financieros destinados a proyectos de investigación en materia de robótica y TIC, incluidas las asociaciones público-privadas, y apliquen en sus políticas de investigación los principios de ciencia abierta e innovación ética responsable; destaca que es necesario destinar recursos suficientes a la búsqueda de soluciones a los retos sociales, éticos, jurídicos y económicos que plantean el desarrollo tecnológico y sus aplicaciones;
7. Pide a la Comisión y a los Estados miembros que fomenten los programas de investigación, que estimulen la investigación sobre los posibles riesgos y

oportunidades de la inteligencia artificial y la robótica a largo plazo y que promuevan cuanto antes un diálogo público estructurado sobre las consecuencias del desarrollo de estas tecnologías; pide a la Comisión que en la revisión intermedia del marco financiero plurianual aumente su apoyo al programa SPARC, financiado por Horizonte 2020; pide a la Comisión y a los Estados miembros que aúnen sus esfuerzos para supervisar detenidamente la transición de estas tecnologías de la investigación a la comercialización y el uso en el mercado y para garantizar que esta transición se produzca de forma fluida, tras las oportunas evaluaciones de su seguridad con arreglo al principio de precaución;

8. Destaca que la innovación en el sector de la robótica y la inteligencia artificial y la integración de esta tecnología en la economía y la sociedad requieren una infraestructura digital que ofrezca una conectividad ubicua; insta a la Comisión a que establezca un marco que satisfaga las necesidades de conectividad del futuro digital de la Unión y que garantice que el acceso a la banda ancha y a las redes 5G sea plenamente acorde con el principio de neutralidad de la red;
9. Está firmemente convencido de que la interoperabilidad entre los sistemas, los dispositivos y los servicios en nube, basada en la seguridad y la privacidad integradas en el diseño, resulta indispensable para los flujos de datos en tiempo real que permiten una mayor flexibilidad y autonomía de los robots y la inteligencia artificial; pide a la Comisión que promueva un entorno abierto que abarque desde las normas abiertas y los modelos de licencia innovadores hasta las plataformas abiertas y la transparencia, con el fin de evitar el confinamiento en sistemas privados que limitan la interoperabilidad;

### **Principios éticos**

10. Señala que el potencial de empoderamiento que encierra el recurso a la robótica se ve matizado por una serie de tensiones o posibles riesgos y que debe ser evaluado detenidamente a la luz de la seguridad y la salud humanas; la libertad, la intimidad, la integridad y la dignidad; la



autodeterminación y la no discriminación, y la protección de los datos personales;

11. Considera que el actual marco normativo de la Unión debe actualizarse y completarse, en su caso, por medio de directrices éticas que reflejen la complejidad del ámbito de la robótica y sus numerosas implicaciones sociales, médicas y bioéticas; estima que es preciso un marco ético claro, estricto y eficiente que oriente el desarrollo, diseño, producción, uso y modificación de los robots, a fin de complementar tanto las recomendaciones jurídicas expuestas en el presente informe como el acervo nacional y de la Unión en vigor; propone, en el anexo a la presente Resolución, un marco en forma de carta integrada por un código de conducta para los ingenieros en robótica, un código deontológico destinado a los comités de ética de la investigación para la revisión de los protocolos de robótica, y licencias tipo para los diseñadores y los usuarios;
12. Pone de relieve el 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; considera que siempre debe ser posible reducir los cálculos del sistema de inteligencia artificial a una forma comprensible para los humanos; estima que los robots avanzados deberían estar equipados con una «caja negra» que registre los datos de todas las operaciones efectuadas por la máquina, incluidos, en su caso, los pasos lógicos que han conducido a la formulación de sus decisiones;
13. Señala que este marco de orientaciones éticas debe basarse en los principios de beneficencia, no maleficencia, autonomía y justicia, así como en los principios consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, como la dignidad humana, la igualdad, la justicia y la equidad, la no discriminación, el consentimiento informado, la vida privada y familiar y la protección de datos, así como en otros principios y valores inherentes al Derecho de la Unión, como la no estigmatización, la transparencia, la autonomía, la responsabilidad individual, y la responsabilidad social, sin olvidar las actuales prácticas y códigos éticos;

14. Considera que se debe prestar especial atención a los robots que representan una amenaza significativa para la privacidad debido a su ubicación en espacios tradicionalmente protegidos y privados y a su capacidad para obtener y transmitir información y datos personales y sensibles;

### **Una agencia europea**

15. Considera necesaria una cooperación reforzada entre los Estados miembros y la Comisión para garantizar normas transfronterizas coherentes en la Unión que fomenten la colaboración entre las industrias europeas y permitan el despliegue en toda la Unión de robots que cumplan los niveles requeridos de seguridad y los principios éticos consagrados en el Derecho de la Unión;
16. Pide a la Comisión que estudie la posibilidad de designar una agencia europea para la robótica y la inteligencia artificial que proporcione los conocimientos técnicos, éticos y normativos necesarios para apoyar la labor de los actores públicos pertinentes, tanto a nivel de la Unión como a nivel de los Estados miembros, en su labor de garantizar una respuesta rápida, ética y fundada ante las nuevas oportunidades y retos —sobre todo los de carácter transfronterizo— que plantea el desarrollo tecnológico de la robótica, por ejemplo en el sector del transporte;
17. Considera justificado, en vista del potencial de la robótica, de los problemas que suscita y de la actual dinámica de inversiones, que esa agencia europea esté dotada de un presupuesto adecuado y de un personal compuesto por reguladores y por expertos externos en cuestiones técnicas y deontológicas dedicados a controlar, desde un punto de vista intersectorial y pluridisciplinar, las aplicaciones basadas en la robótica, a determinar las normas en materia de mejores prácticas y, en su caso, a recomendar medidas reguladoras, a definir nuevos principios y a hacer frente a posibles problemas de protección de los consumidores y desafíos sistémicos; pide a la Comisión (y a la agencia europea, en el caso de que se cree) que informen anualmente al Parlamento sobre los últimos avances de la robótica, así como sobre las medidas que resulten necesarias;

## **Derechos de propiedad intelectual y flujo de datos**

18. Constata que no hay ninguna disposición jurídica que se aplique específicamente a la robótica, pero que las doctrinas y los regímenes jurídicos actuales pueden aplicarse fácilmente a esta, aunque algunos aspectos requieran especial consideración; pide a la Comisión que apoye un enfoque horizontal y de neutralidad tecnológica para la propiedad intelectual en los distintos sectores en que se pueda utilizar la robótica;
19. Pide a la Comisión y a los Estados miembros que velen por que la legislación civil en el sector de la robótica se ajuste al Reglamento general de protección de datos y a los principios de necesidad y proporcionalidad; pide a la Comisión y a los Estados miembros que tengan en cuenta la rápida evolución tecnológica en el ámbito de la robótica, incluidos los avances de los sistemas ciberfísicos, y que velen por que la legislación de la Unión no quede a la zaga del desarrollo y el despliegue tecnológicos;
20. Recalca que el derecho a la protección de la vida privada y el derecho a la protección de los datos personales, consagrados en los artículos 7 y 8 de la Carta y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), son de aplicación en todos los ámbitos de la robótica, y que debe respetarse plenamente el marco jurídico de la Unión en materia de protección de datos; pide, en este contexto, que se revisen las normas y criterios aplicables al uso de cámaras y sensores en los robots; pide a la Comisión que vele por la observancia de los principios de la protección de datos, como la protección de la intimidad desde el diseño y por defecto, la minimización de datos y la limitación de la finalidad, así como por la existencia de mecanismos de control transparentes y vías de recurso adecuadas de conformidad con el Derecho de la Unión en materia de protección de datos, y por que se promuevan recomendaciones y normas adecuadas para ser incorporadas a las políticas de la Unión;
21. Subraya que el libre flujo de datos es fundamental para la economía digital y para el desarrollo en el sector de la robótica y la inteligencia artificial; pone de relieve que un alto grado de seguridad de los sistemas robóticos, incluidos sus sistemas internos de datos y flujos de datos, es crucial para una utilización adecuada de la robótica y la inteligencia artificial; destaca

que ha de garantizarse la protección de las redes de robots y sistemas de inteligencia artificial interconectados para evitar posibles quiebras de la seguridad; recalca que un elevado nivel de seguridad y protección de los datos personales y el debido respeto de la intimidad son esenciales para la comunicación entre los seres humanos y los robots y la inteligencia artificial; resalta la responsabilidad de los diseñadores de robótica e inteligencia artificial de desarrollar productos que sean seguros, fiables y que cumplan su función; pide a la Comisión y a los Estados miembros que apoyen e incentiven el desarrollo de la tecnología necesaria, incluida la seguridad desde el diseño;

### **Normalización, seguridad y protección**

22. Pone de relieve que definir normas y posibilitar la interoperabilidad es fundamental para la competencia futura en el ámbito de la inteligencia artificial y las tecnologías robóticas; pide a la Comisión que continúe trabajando por la armonización internacional de las normas técnicas, en particular junto con los organismos europeos de normalización y la Organización Internacional de Normalización, a fin de fomentar la innovación, evitar la fragmentación del mercado interior y garantizar un elevado nivel de seguridad de los productos y protección de los consumidores, también, en su caso, mediante normas mínimas de seguridad adecuadas para el entorno de trabajo; destaca la importancia de la licitud de la ingeniería inversa y las normas abiertas, para maximizar el valor de la innovación y garantizar que los robots puedan comunicarse entre sí; acoge favorablemente, en este sentido, la creación de comités técnicos especiales, como el ISO/TC 299 Robótica, dedicados exclusivamente a la elaboración de normas sobre robótica;

23. Subraya que los ensayos de robots en situaciones reales es esencial para determinar y evaluar los riesgos que puedan entrañar, así como para su desarrollo tecnológico más allá de la mera fase experimental en el laboratorio; subraya, a este respecto, que los ensayos de robots en situaciones reales, en particular, en ciudades y carreteras, plantean numerosos problemas, incluidos obstáculos que ralentizan el desarrollo de estas fases de ensayo, y requieren un mecanismo de seguimiento eficaz;

pide a la Comisión la elaboración de criterios uniformes para todos los Estados miembros, que estos deberán aplicar para determinar los ámbitos en que se permiten los experimentos con robots de conformidad con el principio de precaución;

## **Medios de transporte autónomos**

### **a) Vehículos autónomos**

24. Subraya que el transporte autónomo abarca todas las formas del transporte por carretera, ferroviario, por vías navegables y aéreo pilotadas a distancia, automatizadas, conectadas y autónomas, incluidos los vehículos, los trenes, los buques, los transbordadores, las aeronaves y los drones, así como todas las futuras formas que resulten del desarrollo y la innovación en este sector;
25. Considera que el sector del automóvil es el que precisa más urgentemente de normas de la Unión y mundiales que garanticen el desarrollo transfronterizo de los vehículos autónomos y automatizados con el fin de explotar plenamente su potencial económico y beneficiarse de los efectos positivos de las tendencias tecnológicas; subraya que la fragmentación de los enfoques normativos podría obstaculizar la implantación de los sistemas de transporte autónomos y poner en peligro la competitividad europea;
26. Pone de relieve que, en el caso de una toma de control imprevista del vehículo, el tiempo de reacción del conductor tiene una importancia capital, y pide, por tanto, a las partes interesadas que prevean valores realistas que determinen los aspectos de seguridad y responsabilidad;
27. Considera que la transición a los vehículos autónomos repercutirá en los siguientes aspectos: la responsabilidad civil (responsabilidad y seguros), la seguridad vial, todas las cuestiones relativas al medio ambiente (por ejemplo, eficiencia energética, uso de tecnologías renovables y fuentes de energía), las cuestiones relativas a los datos (por ejemplo, acceso a los datos, protección de los datos personales y la intimidad, intercambio de datos), las cuestiones relativas a la infraestructura TIC (por ejemplo, alta densidad de

comunicaciones eficientes y fiables) y el empleo (por ejemplo, creación y pérdida de puestos de trabajo, formación de los conductores de vehículos pesados para el uso de vehículos automatizados); subraya que se necesitarán inversiones considerables en las infraestructuras viarias, energéticas y de TIC; pide a la Comisión que examine los aspectos mencionados en sus trabajos sobre los vehículos autónomos;

28. Subraya la importancia decisiva que para la implantación de vehículos autónomos tiene la fiabilidad de la información de posición y tiempo proporcionada por los programas europeos de navegación por satélite Galileo y EGNOS; insta, en este contexto, a que se pongan a punto y se lancen lo antes posible los satélites necesarios para completar el sistema europeo de posicionamiento Galileo;
29. Pone de relieve el gran valor añadido de los vehículos autónomos para las personas con movilidad reducida, puesto que mejoran su participación en el transporte individual por carretera y, de ese modo, hacen más fácil su vida cotidiana;

#### **b) Drones**

30. Reconoce los avances positivos en la tecnología de los drones, en particular en el ámbito de la búsqueda y el salvamento; subraya la importancia de un marco europeo del uso de drones para preservar la seguridad y la intimidad de los ciudadanos de la Unión, y pide a la Comisión que realice un seguimiento de las recomendaciones hechas en la Resolución del Parlamento Europeo, de 29 de octubre de 2015, sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS), comúnmente conocidos como vehículos aéreos no tripulados (UAV), en el ámbito de la aviación civil (5); insta a la Comisión a que realice evaluaciones de los problemas de seguridad relacionados con el uso generalizado de drones; pide a la Comisión que estudie la necesidad de introducir un sistema obligatorio de seguimiento e identificación de los RPAS que permita conocer en tiempo real su posición en vuelo; recuerda que deben garantizarse la homogeneidad y la seguridad de las aeronaves sin

tripulación mediante las medidas establecidas en el Reglamento (CE) n.º 216/2008 del Parlamento Europeo y del Consejo (6);

### **Robots asistenciales**

31. Subraya que, con el tiempo, la investigación y el desarrollo de robots de asistencia geriátrica han pasado a ser más habituales y menos costosos, ofreciendo productos con mayor funcionalidad y mejor aceptación entre los consumidores; pone de relieve la amplia gama de usos de estas tecnologías para ejercer funciones de prevención, asistencia, seguimiento, estimulación y compañía de las personas de edad avanzada o que padecen demencia, trastornos cognitivos y pérdida de memoria;
32. Señala que el contacto humano es uno de los aspectos fundamentales de la atención a las personas; considera que sustituir el factor humano por robots podría deshumanizar la prestación de cuidados, pero, por otra parte, reconoce que los robots podrían realizar las tareas automatizadas de quienes prestan cuidados, aumentando la atención prestada por seres humanos y haciendo más selectivo el proceso de rehabilitación, lo que permitiría al personal médico y asistencial dedicar más tiempo al diagnóstico y a opciones de tratamiento mejor planificadas; destaca que, a pesar del potencial de la robótica para mejorar la movilidad y la integración de las personas con discapacidad o de edad avanzada, seguirán siendo necesarios cuidadores humanos, que ofrecen una importante fuente de interacción social imposible de sustituir en su integridad;

### **Robots médicos**

33. Subraya la importancia de una educación, una formación y una preparación adecuadas de los profesionales de la salud, como médicos y auxiliares sanitarios, con el fin de garantizar el nivel más elevado posible de competencia profesional y proteger y salvaguardar la salud de los pacientes; hace hincapié en la necesidad de definir los requisitos profesionales mínimos que deberá cumplir un cirujano para operar y estar autorizado a utilizar robots quirúrgicos; considera fundamental que se respete el principio de autonomía supervisada de los robots, en virtud del cual la programación inicial de los cuidados y la elección final sobre la

ejecución pertenecen en todo caso al ámbito de decisión de un cirujano humano; subraya la especial importancia que reviste la formación de los usuarios para que puedan familiarizarse con los requisitos tecnológicos en este ámbito; llama la atención acerca de la creciente tendencia al autodiagnóstico mediante el uso de robots móviles y, por consiguiente, de la necesidad de formar a los médicos para que puedan tratar los casos de autodiagnóstico; considera que la utilización de estas tecnologías no debería disminuir ni perjudicar la relación entre médico y paciente, sino proporcionar al médico una asistencia para el diagnóstico y/o el tratamiento de los paciente, con el fin de reducir el riesgo de error humano y aumentar la calidad y la esperanza de vida;

34. Considera que los robots en medicina avanzan cada vez más en la ejecución de cirugías de alta precisión y en la realización de procedimientos repetitivos, y que pueden mejorar los resultados de la rehabilitación y proporcionar un apoyo logístico sumamente eficaz en los hospitales; señala que los robots médicos tienen también el potencial de reducir los gastos sanitarios, permitiendo al personal médico desviar su atención del tratamiento a la prevención, así como de liberar más recursos presupuestarios para adaptarse mejor a las diversas necesidades de los pacientes, para la formación continua de los profesionales sanitarios y para la investigación;
35. pide a la Comisión que garantice la seguridad de los procedimientos utilizados para ensayar nuevos dispositivos robóticos médicos, en particular en el caso de los dispositivos (7) que se implanten en el cuerpo humano, antes de la fecha de entrada en vigor del Reglamento;

### **Rehabilitación e intervenciones en el cuerpo humano**

36. Constata los grandes progresos de la robótica, así como su potencial futuro en el ámbito de la rehabilitación de órganos dañados y el restablecimiento de funciones corporales reducidas, si bien es consciente de las complejas cuestiones que ello suscita, en particular por las posibilidades de intervención en el cuerpo humano, en la medida en que los robots médicos y, en particular, los sistemas ciberfísicos (SCF) pueden modificar sustancialmente nuestras concepciones en torno al cuerpo humano sano,



en cuanto que pueden llevarse o implantarse directamente en el cuerpo humano; destaca la importancia que reviste establecer con carácter de urgencia comités de ética sobre robótica en los hospitales y otras instituciones sanitarias, debidamente dotados con el personal apropiado y encargados de examinar y contribuir a resolver problemas éticos inusuales y complejos relacionados con cuestiones que afecten al cuidado y el tratamiento de los pacientes; pide a la Comisión y a los Estados miembros que desarrollen directrices para ayudar al establecimiento y funcionamiento de dichos comités;

37. Señala que, en el ámbito de aplicaciones médicas vitales, como las prótesis robóticas, debe garantizarse el acceso continuo y sostenible al mantenimiento, la mejora y, en particular, las actualizaciones de software que subsanan fallos y vulnerabilidades;
38. Recomienda la creación de entidades de confianza independientes con el fin de retener los medios necesarios para proporcionar a las personas que lleven dispositivos médicos vitales y avanzados los servicios que precisan, como mantenimiento, reparaciones y mejoras, incluidas actualizaciones de software, especialmente cuando el proveedor original deje de prestar dichos servicios; sugiere que se prevea la obligación de que los fabricantes proporcionen instrucciones de diseño global, incluido el código fuente, a estas entidades de confianza independientes, de forma similar al depósito legal de publicaciones en una biblioteca nacional;
39. Señala los riesgos de la manipulación o la desconexión de SCF integrados en el cuerpo humano o del borrado de su memoria, ya que ello podría poner en peligro la salud humana, o en un caso extremo incluso la vida del ser humano, y por ello destaca la prioridad de que se protejan tales sistemas;
40. Destaca la importancia de garantizar el acceso en pie de igualdad para todos a estas innovaciones tecnológicas, a los instrumentos y a las intervenciones de que se trata; pide a la Comisión y a los Estados miembros que promuevan el desarrollo de tecnologías de apoyo, con el fin de promover el desarrollo y la adopción de estas tecnologías por parte de los individuos que las necesiten, de conformidad con el artículo 4 de la Convención de las

Naciones Unidas sobre los derechos de las personas con discapacidad, de la que la Unión es signataria;

### **Educación y empleo**

41. Llama la atención sobre las previsiones de la Comisión según las cuales podría tener que hacer frente hasta el año 2020 a una escasez de hasta 825 000 profesionales en el sector de las TIC, a la vez que el 90 % de los puestos de trabajo requerirá al menos unas capacidades digitales básicas; acoge con satisfacción la iniciativa de la Comisión de proponer un plan de trabajo para la posible utilización y revisión del marco de competencias digitales y de los descriptores de competencias digitales para todos los niveles de aprendizaje, e insta a la Comisión a que preste un apoyo significativo al desarrollo de las competencias digitales en todos los grupos de edad, con independencia de la categoría profesional, como un primer paso hacia una mejor adaptación de la oferta y la demanda en el mercado laboral; destaca que el crecimiento de la robótica exige que los Estados miembros desarrollen sistemas de formación y educación más flexibles con el fin de garantizar que las estrategias relativas al desarrollo de las capacidades se ajustan a las necesidades de la economía de los robots;
42. Considera que la industria digital, las propias mujeres y la economía europea saldrían ganando si se consiguiera que más mujeres jóvenes se decantaran por una carrera digital y se contrataran más mujeres en empleos digitales; pide a la Comisión y a los Estados miembros que emprendan iniciativas dirigidas a apoyar a las mujeres en el sector de las TIC y a mejorar su capacitación en el ámbito digital;
43. Pide a la Comisión que empiece a analizar y supervisar más estrechamente la evolución a medio y largo plazo del empleo, con especial énfasis en la creación, la deslocalización y la pérdida de puestos de trabajo en los diferentes campos/ámbitos de calificación, con el fin de determinar en qué ámbitos se está creando empleo y en cuáles se está perdiendo como consecuencia de la mayor utilización de los robots;
44. Destaca la importancia que reviste la previsión de los cambios sociales, habida cuenta de los efectos que podrían tener el desarrollo y la

implantación de la robótica y la inteligencia artificial; pide a la Comisión que analice los diferentes posibles escenarios y sus consecuencias para la viabilidad de los sistemas de seguridad social en los Estados miembros; considera que debería emprenderse un debate integrador sobre los nuevos modelos de empleo y sobre la sostenibilidad de nuestros sistemas tributarios y sociales tomando como base unos ingresos suficientes, incluida la posible introducción de una renta básica mínima;

45. Destaca la importancia que revisten la flexibilidad de las competencias y de las habilidades sociales, creativas y digitales en la educación; está convencido de que, además de los conocimientos académicos impartidos en las centros escolares, al tiempo que considera que el aprendizaje a lo largo de toda la vida presupone también la acción a lo largo de toda la vida;
46. Constata el enorme potencial de la robótica a la hora de mejorar la seguridad en el entorno laboral mediante la transferencia a los robots de una serie de tareas peligrosas y perjudiciales que desempeñan actualmente los seres humanos, al tiempo que advierte del peligro que podría entrañar la robotización en el sentido de crear una serie de nuevos riesgos como consecuencia del creciente número de interacciones entre los seres humanos y los robots en el lugar de trabajo; subraya a este respecto la importancia de aplicar normas estrictas y orientadas hacia el futuro que regulen las interacciones entre los seres humanos y los robots, a fin de garantizar la salud, la seguridad y el respeto de los derechos fundamentales en el lugar de trabajo;

### **Efecto sobre el medio ambiente**

47. Señala que el desarrollo de la robótica y la inteligencia artificial debería realizarse de tal manera que se limite el impacto en el medio ambiente mediante un consumo de energía eficaz, la eficiencia energética mediante el fomento del uso de energías renovables y de materiales escasos, la generación de residuos mínimos —en particular, residuos eléctricos y electrónicos— y la reparabilidad. pide, por tanto, a la Comisión que incorpore los principios de una economía circular a toda política de la Unión sobre robótica; señala que el uso de la robótica tendrá también un efecto positivo en el medio ambiente, en especial en los sectores de la

agricultura, el abastecimiento alimentario y el transporte, ya que reducirá en particular el tamaño de la maquinaria y el uso de abonos, energía y agua, y desarrollará la agricultura de precisión y la optimización de los circuitos de distribución;

48. Destaca que los SCF tendrán como resultado la creación de sistemas de energía e infraestructura que podrán controlar el flujo de electricidad del productor al consumidor, así como la creación de «prosumidores» energéticos que producirán y consumirán energía, lo que redundará en importantes beneficios para el medio ambiente;

### **Responsabilidad**

49. Considera que la responsabilidad civil por los daños y perjuicios causados por robots es una cuestión fundamental que también debe analizarse y abordarse a escala de la Unión, con el fin de garantizar el mismo grado de eficiencia, transparencia y coherencia en la garantía de la seguridad jurídica en toda la Unión Europea en beneficio de los ciudadanos, los consumidores y las empresas;
50. Observa que el desarrollo de la tecnología robótica requerirá una mayor comprensión de las bases comunes necesarias para la actividad conjunta humano-robótica, que debe basarse en dos relaciones de interdependencia básicas, como la previsibilidad y la direccionalidad; señala que estas dos relaciones de interdependencia son fundamentales para determinar qué información debe ser compartida entre seres humanos y robots y cómo puede conseguirse una base común entre seres humanos y robots que permita una acción conjunta humano-robótica eficaz;
51. Pide a la Comisión que presente, sobre la base del artículo 114 del TFUE, una propuesta de instrumentos legislativos sobre los aspectos jurídicos relacionados con el desarrollo y el uso de la robótica y la inteligencia artificial previsibles en los próximos diez o quince años, junto con instrumentos no legislativos —por ejemplo, directrices y códigos de conducta—, tal como los que se mencionan en las recomendaciones que figuran en el anexo;

52. Considera que, independientemente del instrumento jurídico futuro que se escoja en materia de responsabilidad civil por los daños y perjuicios causados por robots en casos distintos a los perjuicios patrimoniales, dicho instrumento legislativo no debería en modo alguno limitar el tipo o el alcance de los daños y perjuicios que puedan ser objeto de compensación, ni tampoco limitar la naturaleza de dicha compensación, por el único motivo de que los daños y perjuicios hayan sido causados por un agente no perteneciente a la especie humana;
53. Considera que el futuro instrumento legislativo debe basarse en una evaluación en profundidad realizada por la Comisión que determine si debe aplicarse el enfoque de la responsabilidad objetiva o el de gestión de riesgos;
54. Señala al mismo tiempo que la responsabilidad objetiva únicamente exige probar que se ha producido un daño o perjuicio y el establecimiento de un nexo causal entre el funcionamiento perjudicial del robot y los daños o perjuicios causados a la persona que los haya sufrido;
55. Observa que el enfoque de gestión de riesgos no se centra en la persona «que actuó de manera negligente» como personalmente responsable, sino en la persona que es capaz, en determinadas circunstancias, de minimizar los riesgos y gestionar el impacto negativo;
56. Considera que, en principio, una vez que las partes en las que incumba la responsabilidad última hayan sido identificadas, dicha responsabilidad debería ser proporcional al nivel real de las instrucciones impartidas a los robots y a su grado de autonomía, de forma que cuanto mayor sea la capacidad de aprendizaje o la autonomía y cuanto más larga haya sido la «formación» del robot, mayor debiera ser la responsabilidad de su formador; observa en particular que, al determinar a quién incumbe realmente la responsabilidad de los daños o perjuicios causados por un robot, las competencias adquiridas a través de la «formación» de un robot no deberían confundirse con las competencias estrictamente dependientes de su capacidad de aprender de modo autónomo; señala que, al menos en la etapa actual, la responsabilidad debe recaer en un humano, y no en un robot;

57. Señala que una posible solución a la complejidad de la asignación de responsabilidad por los daños y perjuicios causados por robots cada vez más autónomos, podría ser el establecimiento de un régimen de seguro obligatorio, como ya se aplica, por ejemplo, en el caso de los automóviles; observa no obstante que, a diferencia del régimen de seguros en la circulación por carretera, en el que el seguro cubre tanto las actuaciones humanas como los fallos mecánicos, un sistema de seguros para robots debería tener en cuenta todas las responsabilidades potenciales en la cadena;
58. Considera que, tal como sucede con el seguro de vehículos de motor, dicho sistema podría completarse con un fondo que garantizara la reparación de daños en los casos de ausencia de una cobertura de seguro; pide al sector de los seguros que desarrolle nuevos productos y tipos de ofertas adaptados a los progresos de la robótica;
59. Pide a la Comisión que, cuando realice una evaluación de impacto de su futuro instrumento legislativo, explore, analice y considere las implicaciones de todas las posibles soluciones jurídicas, tales como:
- a) establecer un régimen de seguro obligatorio en los casos en que sea pertinente y necesario para categorías específicas de robots, similar al existente para los automóviles, en el que los fabricantes o los propietarios de robots estarían obligados a suscribir un contrato de seguro por los posibles daños y perjuicios causados por sus robots.
  - b) establecer un fondo de compensación que no solo garantice la reparación de los daños o perjuicios causados por un robot ante la ausencia de un seguro;
  - c) permitir que el fabricante, el programador, el propietario o el usuario puedan beneficiarse de un régimen de responsabilidad limitada si contribuyen a un fondo de compensación o bien si suscriben conjuntamente un seguro que garantice la compensación de daños o perjuicios causados por un robot;

- d) decidir si conviene crear un fondo general para todos los robots autónomos inteligentes o crear un fondo individual para cada categoría de robot, así como la elección entre un canon único al introducir el robot en el mercado o pagos periódicos durante la vida del robot;
- e) crear un número de matrícula individual que figure en un registro específico de la Unión que asegure la asociación entre el robot y el fondo del que depende y que permita que cualquier persona que interactúe con el robot esté al corriente de la naturaleza del fondo, los límites de su responsabilidad en caso de daños materiales, los nombres y las funciones de los participantes y otros datos pertinentes;
- f) crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas 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.
- g) introducir un instrumento específico para los consumidores que deseen reclamar de forma colectiva una reparación por los daños y perjuicios derivados del incorrecto funcionamiento de máquinas inteligentes a las empresas productoras responsables;

### **Aspectos internacionales**

60. Constata que no es necesario modificar de forma sustantiva y con carácter de urgencia las actuales normas de Derecho internacional privado en materia de accidentes de tráfico aplicables en la Unión para adaptarlas al desarrollo de los vehículos autónomos, si bien considera que la simplificación del actual sistema dual con el que se determina la legislación aplicable (basado en el Reglamento (CE) n.º 864/2007 del Parlamento Europeo y del Consejo (8) y el Convenio de La Haya de 4 de mayo de 1971 sobre la ley aplicable en materia de accidentes de circulación por carretera) podría mejorar la

seguridad jurídica y limitar las posibilidades de búsqueda del foro más favorable;

61. Señala la necesidad de introducir modificaciones a algunos acuerdos internacionales, como el Convenio de Viena sobre la circulación vial, de 8 de noviembre de 1968, y el Convenio de la Haya sobre la ley aplicable en materia de accidentes de circulación por carretera;
62. Espera que la Comisión vele por que los Estados miembros apliquen de manera uniforme la ley internacional, por ejemplo el Convenio de Viena sobre la circulación vial, cuya modificación es necesaria, a fin de hacer posible el transporte sin conductor, y pide a la Comisión, a los Estados miembros y al sector que apliquen con la mayor brevedad posible los objetivos de la Declaración de Ámsterdam;
63. Alienta encarecidamente a la comunidad internacional a cooperar para estudiar los desafíos sociales, éticos y jurídicos y, seguidamente, a establecer normas reglamentarias bajo las auspicios de las Naciones Unidas;
64. Destaca que las restricciones y condiciones establecidas en el Reglamento (CE) n.º 428/2009 del Parlamento Europeo y del Consejo (9) sobre el comercio de los productos de doble uso (productos, programas informáticos y tecnología que puedan utilizarse para aplicaciones tanto civiles como militares o que puedan contribuir a la proliferación de armas de destrucción masiva) deberían extenderse a las aplicaciones de la robótica;

### **Aspectos finales**

65. Pide a la Comisión, sobre la base del artículo 225 del TFUE, que presente una propuesta de Directiva, sobre la base del artículo 114 del TFUE, relativa a las normas de legislación civil en materia de robótica, siguiendo las recomendaciones detalladas que figuran en el anexo;
66. Constata que estas recomendaciones respetan los derechos fundamentales y el principio de subsidiariedad;



67. Opina que la propuesta solicitada tendría implicaciones financieras si se procede a la creación de una nueva agencia europea;
68. Encarga a su Presidente que transmita la presente propuesta y las recomendaciones que se detallan en el anexo a la Comisión y al Consejo.

---

(1) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

(2) 1.<sup>a</sup> Un robot no hará daño a un ser humano ni permitirá que, por inacción, este sufra daño. 2.<sup>a</sup> 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.<sup>a</sup> Un robot protegerá su propia existencia en la medida en que dicha protección no entre en conflicto con las leyes primera y segunda (véase Isaac Asimov, *Círculo vicioso* (*Runaround*), 1943) y 0.<sup>a</sup> Un robot no hará daño a la humanidad ni permitirá que, por inacción, esta sufra daño.

(3) Véase la Declaración Schuman de 1950: «Europa no se hará de una vez ni en una obra de conjunto. Se hará gracias a realizaciones concretas, que creen en primer lugar una solidaridad de hecho».

(4) Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (DO L 210 de 7.8.1985, p. 29).

(5) Textos Aprobados, P8\_TA(2015)0390.

(6) Reglamento (CE) n.º 216/2008, del Parlamento Europeo y del Consejo, de 20 de febrero de 2008, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia Europea de Seguridad Aérea, y se deroga la Directiva 91/670/CEE del Consejo, el Reglamento (CE) n.º 1592/2002 y la Directiva 2004/36/CE (DO L 79 de 19.3.2008, p. 1).

(7) Véase la Resolución legislativa del Parlamento Europeo, de 2 de abril de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre los productos sanitarios y por el que se modifican la Directiva

2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 (COM(2012)0542 – C7-0318/2012 – 2012/0266(COD)).

(8) Reglamento (CE) n.º 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales (Roma II) (DO L 199 de 31.7.2007, p. 40.).

(9) Reglamento (CE) n.º 428/2009 del Consejo por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso (DO L 341 de 29.5.2009, p. 1).

## **ANEXO A LA PROPUESTA DE RESOLUCIÓN: RECOMENDACIONES DETALLADAS RESPECTO AL CONTENIDO DE LA PROPUESTA SOLICITADADA**

### **Definición y clasificación de los «robots inteligentes»**

Debe establecerse una definición europea común de robots autónomos «inteligentes», cuando proceda, incluidas las definiciones de sus subcategorías, teniendo en cuenta las siguientes características:

- la capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos;
- la capacidad de aprender a través de la experiencia y la interacción;
- la forma del soporte físico del robot;
- la capacidad de adaptar su comportamiento y acciones al entorno.

### **Registro de los «robots inteligentes»**

A efectos de la trazabilidad y para facilitar la aplicación de nuevas recomendaciones, cabe introducir un sistema de registro de robots avanzados, basado en los criterios establecidos para la clasificación de los robots. Tanto el sistema de registro como el propio registro deberían establecerse a escala de la Unión, de forma que cubran el mercado interior, y podrían ser gestionados por una agencia designada de la Unión para la robótica y la inteligencia artificial en el caso de que se procediera a la creación de dicha agencia.

### **Responsabilidad civil**

Cualquier solución jurídica elegida en materia de responsabilidad de los robots y de la inteligencia artificial para los supuestos diferentes de los daños materiales no debería en modo alguno limitar el tipo o el alcance de los daños y perjuicios que puedan ser objeto de compensación, y tampoco debería limitar la naturaleza

de dicha compensación, basándose únicamente en que los daños han sido causados por un agente no perteneciente a la especie humana.

El futuro instrumento legislativo debe basarse en una evaluación en profundidad realizada por la Comisión que defina si debe aplicarse el enfoque de la responsabilidad objetiva o el de gestión de riesgos;

Sería conveniente establecer un régimen de seguro obligatorio, que podría basarse en la obligación del productor de suscribir un seguro para los robots autónomos por él fabricados.

El sistema de seguro debería complementarse con un fondo para garantizar la compensación de los daños y perjuicios en los supuestos en los que no exista una cobertura de seguro.

Cualquier decisión política sobre las normas de responsabilidad civil aplicables a robots e inteligencia artificial debería adoptarse tras consultar un proyecto de investigación y desarrollo a escala europea especializado en robótica y neurociencia, de manera que los científicos y los expertos sean capaces de evaluar todos los riesgos y las consecuencias asociados;

### **Interoperabilidad, acceso al código fuente y derechos de propiedad intelectual**

Cabría garantizar la interoperabilidad de los robots autónomos conectados a la red autónoma que interactúan entre sí. El acceso al código fuente, a los datos de entrada y a los detalles de construcción debería estar disponible cuando fuera necesario, para investigar tanto los accidentes como los daños causados por «robots inteligentes», así como para velar por su funcionamiento, disponibilidad, fiabilidad, seguridad y protección continuados.

### **Carta sobre robótica**

Cuando formule propuestas legislativas relativas a la robótica, la Comisión debería tener en cuenta los principios recogidos en la siguiente Carta sobre robótica.

## **CARTA SOBRE ROBÓTICA**

La propuesta de un código de conducta ética en el campo de la robótica sentará las bases para la identificación, la supervisión y el cumplimiento de los principios éticos fundamentales desde la fase de diseño y desarrollo.

El marco, elaborado tras consultar un proyecto de investigación y desarrollo a escala europea especializado en robótica y neurociencia, debe concebirse de un modo reflexivo que permita efectuar ajustes individuales caso por caso para evaluar si un determinado comportamiento es adecuado o equivocado en una situación determinada y tomar decisiones conforme a una jerarquía de valores preestablecidos.

El código no debería reemplazar la necesidad de abordar los principales retos jurídicos en este ámbito, sino que ha de tener una función complementaria. Facilitará más bien, la categorización ética de la robótica, reforzará los esfuerzos de innovación responsable en este ámbito y responderá a las preocupaciones de los ciudadanos.

Convendría hacer especial hincapié en las fases de investigación y desarrollo de la trayectoria tecnológica pertinente (proceso de concepción, análisis ético, controles de auditoría, etc.). El código de conducta debería tener como objetivo no solo la necesidad de abordar la necesidad de cumplimiento de determinadas normas éticas por parte de investigadores, profesionales, usuarios y diseñadores, sino también de introducir un procedimiento para la resolución de los dilemas éticos y permitir que estos sistemas puedan funcionar de una manera éticamente responsable.

## **CÓDIGO DE CONDUCTA ÉTICA PARA LOS INGENIEROS EN ROBÓTICA**

### **PREÁMBULO**

El código de conducta invita a todos los investigadores y diseñadores a actuar de forma responsable y con la máxima consideración a la necesidad de respetar la dignidad, intimidad y la seguridad de las personas.

El código pide una estrecha colaboración entre todas las disciplinas a fin de garantizar que se lleve a cabo la investigación en robótica en la Unión de un modo seguro, ético y eficaz.

El código de conducta cubre todas las actividades de investigación y desarrollo en el campo de la robótica.

El código de conducta es voluntario y ofrece un conjunto de principios generales y directrices para las medidas que adopten todas las partes interesadas.

Se invita a los organismos de financiación en materia de robótica, los centros de investigación, los investigadores y los comités de ética a que examinen desde las primeras etapas, las consecuencias futuras de las tecnologías u objetos que se investigan y de crear una cultura de la responsabilidad para hacer frente a los retos y oportunidades que puedan plantearse en el futuro.

Los organismos públicos y privados de financiación de la investigación en el ámbito de la robótica deberían exigir la realización y presentación de una evaluación del riesgo para cada propuesta de financiación de la investigación en la materia. Un código de estas características debería considerar que la responsabilidad incumbe a los seres humanos, no a los robots.

**Los investigadores en el campo de la robótica deberían comprometerse a adoptar una conducta estricta en materia de ética y de deontología así como a respetar los siguientes principios:**

Beneficencia — los robots deben actuar en beneficio del hombre;

Principio de no perjuicio o maleficencia — la doctrina de «primero, no hacer daño», en virtud del cual los robots no deberían perjudicar a las personas;

Autonomía — la capacidad de tomar una decisión con conocimiento de causa e independiente sobre los términos de interacción con los robots;

Justicia — la distribución justa de los beneficios asociados a la robótica y la asequibilidad de los robots utilizados en el ámbito de la asistencia sanitaria a domicilio y de los cuidados sanitarios en particular.

### **Derechos fundamentales**

Las actividades de investigación en materia de robótica deben respetar los derechos fundamentales; y por su parte, las actividades de concepción, ejecución, difusión y explotación, por su parte, han de estar al servicio del bienestar y la autodeterminación de las personas y de la sociedad en general. La dignidad y la autonomía humanas — tanto físicas como psicológicas — siempre tienen que respetarse.

### **Precaución**

Las actividades de investigación en el ámbito de la robótica deben llevarse a cabo de conformidad con el principio de precaución, anticipándose a los posibles impactos de sus resultados sobre la seguridad y adoptando las precauciones debidas, en función del nivel de protección, al tiempo que se fomenta el progreso en beneficio de la sociedad y del medio ambiente.

### **Participación**

Los ingenieros en robótica garantizan la transparencia y el respeto al derecho legítimo de acceso a la información de todas las partes interesadas. La integración permite la participación en los procesos de toma de decisiones de todas las partes interesadas o afectadas por las actividades de investigación en el ámbito de la robótica.

### **Rendición de cuentas**

Los ingenieros en robótica deben rendir cuentas de las consecuencias sociales y medioambientales y el impacto sobre la salud humana que la robótica puede conllevar para las generaciones presentes y futuras.

### **Seguridad**

Los diseñadores de robots han de tener en cuenta y respetar la integridad física, la seguridad, la salud y los derechos de las personas. Un ingeniero en robótica debe preservar el bienestar sin dejar de respetar los derechos humanos, y divulgar con prontitud los factores susceptibles de poner en peligro a la población o al medio ambiente.

### **Reversibilidad**

La reversibilidad, que es una condición necesaria de la posibilidad de control, es un concepto fundamental en la programación de robots para que se comporten de manera segura y fiable. Un modelo de reversibilidad indica al robot qué acciones son reversibles y, en su caso, el modo de revertirlas. La posibilidad de deshacer la última acción o secuencia de acciones, permite al usuario anular las acciones no deseadas y volver a la fase «buena» de su trabajo.

### **Privacidad**

El derecho a la intimidad debe siempre respetarse. Un ingeniero en robótica debe garantizar que la información privada se conservará en total seguridad y solo se utilizará de forma adecuada. Por otra parte, el ingeniero en robótica ha de garantizar que los individuos no son personalmente identificables, salvo en circunstancias excepcionales, y únicamente en caso de consentimiento claro, consciente e inequívoco. El consentimiento consciente de la persona tiene que solicitarse y recabarse con anterioridad a cualquier interacción hombre-máquina. A tal efecto, los diseñadores en robótica tienen la responsabilidad de desarrollar y aplicar procedimientos para garantizar el consentimiento válido, la confidencialidad, el anonimato, el trato justo y el respeto de la legalidad. Los diseñadores llevarán a cabo todas las solicitudes de destrucción de los datos relacionados y de eliminación de las bases de datos.

### **Maximizar beneficios y reducir al mínimo los daños**

Los investigadores deben intentar maximizar los beneficios de su actividad en todas las fases, desde su concepción hasta su difusión. Es conveniente evitar cualquier daño a los participantes o a los seres humanos que participen en los experimentos, ensayos o estudios en el ámbito de la investigación. En caso de aparición de riesgos inevitables que formen parte de un elemento integrante de



la investigación, sería necesario llevar a cabo una evaluación sólida de los riesgos, desarrollar protocolos de gestión y adecuarse a los mismos. Normalmente, los riesgos a un daño no deberían ser superior a los existentes en la vida cotidiana, es decir, las personas no han de estar expuestas a riesgos mayores o adicionales a aquellos a los que están expuestos en su vida cotidiana. La explotación de un sistema de robótica debería basarse siempre en una profunda evaluación de los riesgos, y reposar en los principios de proporcionalidad y de precaución.

## **CÓDIGO DEONTOLÓGICO PARA LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN**

### **Principios**

#### **Independencia**

El proceso de revisión ética ha de ser independiente de la propia investigación. Este principio pone de relieve la necesidad de evitar conflictos de intereses entre los investigadores y aquellos encargados de revisar el protocolo ético, y entre los revisores y las estructuras de gobernanza organizativa.

#### **Competencia**

Sería conveniente que el proceso de revisión ética fuera efectuado por revisores con experiencia adecuada, teniendo en cuenta la necesidad de un examen cuidadoso de la diversidad en la composición y en la formación específica en materia de ética de los comités de ética de la investigación.

#### **Transparencia y obligación de rendir cuentas**

El proceso de revisión debería ser responsable y en condiciones de ser objeto de control. Los comités de ética de la investigación regionales deben ser conscientes de sus responsabilidades y estar adecuadamente ubicados dentro de estructuras organizativas que les doten de transparencia operativa y de procedimientos destinados a conservar y revisar las normas.

#### **La función de un comité de ética de la investigación**

Normalmente, los comités de ética de la investigación son responsables de revisar toda investigación en la que intervienen participantes humanos realizada por persona empleadas en o por la institución en cuestión; de garantizar que la revisión ética es independiente, competente y oportuna; de proteger la dignidad, los derechos y el bienestar de los sujetos participantes de la investigación; de velar por la seguridad de los investigadores; de tener en cuenta los intereses legítimos de las demás partes interesadas; de hacer juicios razonados del mérito científico de las propuestas; de formular recomendaciones con conocimiento de causa al investigador si la propuesta es considerada insuficiente en determinados aspectos.

### **Constitución de un Comité de Ética de la Investigación**

Un Comité de Ética de la Investigación debería tener normalmente un carácter multidisciplinar: incluir a hombres y mujeres, estar constituido por miembros con una amplia experiencia y conocimientos en el ámbito de la investigación en robótica. El mecanismo de designación debería velar por que los miembros del comité garanticen un equilibrio adecuado entre conocimientos científicos, formación filosófica, ética o jurídica, así como diferentes puntos de vista. Además, debería contar con al menos un miembro con conocimientos especializados en materia de ética y con usuarios de servicios especializados de salud, educación o servicios sociales cuando dichos ámbitos figuren dentro de las actividades de investigación, así como con miembros que dispongan de conocimientos metodológicos específicos relacionados con la investigación que evalúen, de tal forma que se eviten los conflictos de intereses.

### **Control**

Sería conveniente que todos los organismos de investigación establecieran procedimientos adecuados para supervisar la ejecución de la investigación que haya recibido el visto bueno en materia de ética hasta la finalización del mismo, y garantizar una revisión continua en el supuesto de que el diseño de la investigación prevea posibles cambios a lo largo del tiempo que debieran tratarse. Los controles deberían ser proporcionados a la naturaleza y a la intensidad del riesgo vinculado con la investigación. Cuando un comité de ética de la investigación considere que un informe de seguimiento plantea importantes dudas sobre la conducta ética del estudio, deberá solicitar un detalle

pormenorizado y exhaustivo de la investigación con vistas a efectuar un examen ético. Cuando considere que un estudio se está llevando a cabo de una forma contraria a la ética, debería plantearse la retirada de su aprobación y suspenderse o interrumpirse la investigación.

## **LICENCIA PARA LOS DISEÑADORES**

- Los diseñadores deberán tener en cuenta los valores europeos de dignidad, autonomía y autodeterminación, libertad y justicia, antes, durante y después del proceso de concepción, desarrollo y de aplicación de esas tecnologías, incluida la necesidad de no perjudicar, herir, engañar o explorar a los usuarios (vulnerables).
- Los diseñadores deberán introducir principios de diseño de sistemas fiables en todos los aspectos del funcionamiento de un robot, tanto para la concepción del material y de programas informáticos, como para el tratamiento de datos dentro o fuera de la plataforma a efectos de seguridad.
- Los diseñadores deberán introducir dispositivos concebidos para asegurar que las informaciones privadas se conservan con total seguridad y solo se utilizan de manera adecuada.
- Los diseñadores deberán integrar mecanismos de salida evidentes (teclas de interrupción de urgencia) que deberán ser coherentes con los objetivos de diseño razonables.
- Los diseñadores deberán garantizar que un robot funciona de modo conforme a los principios éticos y jurídicos a nivel local, nacional e internacional.
- Los diseñadores deberán asegurarse de que las etapas de toma de decisión del robot puedan ser objeto de reconstrucción y trazabilidad.
- Los diseñadores deberán asegurarse de que es conveniente una transparencia máxima en la programación de los sistemas robóticos, así como la previsibilidad del comportamiento de los robots.

- Los diseñadores deberán analizar la previsibilidad de un sistema humano-robot teniendo en cuenta la incertidumbre en la interpretación y en la acción, así como los posibles fallos de los robots o del hombre.
- Los diseñadores deberán desarrollar instrumentos de rastreo en la fase de concepción del robot. Estos instrumentos permitirán tener en cuenta y explicar los comportamientos de los robots, aunque sea de forma limitada, en los distintos niveles previstos para los expertos, los operadores y los usuarios.
- Los diseñadores deberán elaborar protocolos de concepción y evaluación, y colaborar con los usuarios y las partes interesadas potenciales para evaluar las ventajas y los riesgos de la robótica, incluido a nivel cognitivo, psicológico y medioambiental.
- Los diseñadores deberán asegurarse de que los robots son identificables como tales al relacionarse con seres humanos.
- Los diseñadores deberán salvaguardar la seguridad y la salud de las personas que interactúan y entran en contacto con los robots, teniendo en cuenta que estos, como productos, deberán elaborarse utilizando procesos que garantizan su seguridad y protección. Un ingeniero en robótica ha de preservar el bienestar humano, al tiempo que respeta los derechos humanos, y no podrá accionar un robot sin garantizar la seguridad, la eficacia y la reversibilidad del funcionamiento del sistema.
- Los diseñadores deberán obtener el dictamen favorable de un comité de ética de la investigación antes de probar un robot en un entorno real o implicando a seres humanos en los procedimientos de concepción y desarrollo.

## **LICENCIA PARA LOS USUARIOS**

- Los usuarios estarán autorizados a hacer uso de un robot sin miedo de perjuicio físico o psicológico.

- Los usuarios deben tener derecho a esperar que un robot efectúe las tareas para las que haya sido expresamente concebido.
- Los usuarios deben ser consciente de que los robots pueden tener límites de percepción, límites cognitivos y límites de accionamiento.
- Los usuarios deberán respetar la fragilidad humana, tanto física como psicológica, así como las necesidades emocionales de los seres humanos.
- Los usuarios deben tener en cuenta el derecho a la vida privada de las personas, incluida la desactivación de videomonitores durante procedimientos íntimos.
- Los usuarios no están autorizados a recoger, utilizar o divulgar información personal sin el consentimiento explícito de la persona concernida.
- Los usuarios no están autorizados a utilizar un robot de modo contrario a los principios y normas éticas o jurídicas.
- Los usuarios no están autorizados a modificar los robots para utilizarlos como armas.

**BIBLIOGRAFÍA**

AA.VV.: *E-Abogacía*, CREMADES, J. (coord. jurídico) y BADÍA Y LIBERAL, E. (coord. periodístico), La Ley, Madrid, 2007.

ÁLVAREZ-SALA WALTHER, J.: *El blanqueo de capitales y las profesiones jurídicas*, Ensayos de actualidad de escritura pública, Consejo General del Notariado, Madrid, 2004.

BRUCH MASERAS, E.: "I.A.: qué es, cuál usar y cómo", *Abogacía Española*, núm. 108, febrero 2018, p. 9.

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA: "La intervención de las comunicaciones del imputado con su abogado quien, a su vez, es decano de un colegio", Informe 3/2015, Comisión Jurídica del Consejo General de la Abogacía Española, 28 de julio de 2015.

CORTÉS BECHIARELLI, E.: *El secreto profesional del abogado y el procurador y su proyección penal*, Marcial Pons, Madrid, 1998.

DEL ROSAL, R.: *Normas deontológicas de la Abogacía Española. Una doctrina construida a partir del ejercicio de la competencia disciplinaria*, Civitas, Madrid, 2002.

DE TOMÁS MORALES, S.: "Hacia una cultura de ciberseguridad: capacitación especializada para un «proyecto compartido». Especial referencia la ámbito universitario", *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, núm. 92, mayo-agosto 2014, pp. 13-47.

GUARDIOLA SALMERÓN, M.: "Retos, desafíos y nuevas oportunidades", *Abogacía Española*, núm. 108, febrero 2018, p. 10.

INTERNATIONAL BAR ASSOCIATION: *Privilege and confidentiality*, Londres, 2006.

MOLINA PÉREZ-TOMÉ, S.: "Machine Learning en el sector legal", *Abogacía Española*, núm. 108, febrero 2018, p. 14.

MORELL RAMOS, J.: “La Inteligencia Artificial en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará”, *Abogacía Española*, núm. 108, febrero 2018, pp. 7 y 8.

MULLERAT BALMAÑÁ, R.M.: “Confidente o cancerbero (algunas consideraciones sobre el secreto profesional del abogado)”, *La Ley*, núm. 5783, de 19 de mayo de 2003.

MUÑOZ CONDE, F.: *Derecho Penal. Parte especial*, 12ª ed., Tirant lo Blanch, Valencia, 1999.

PARDO GATO, J.R.: “La abogacía ante el desarrollo de las nuevas tecnologías”, en el libro del VIII Congreso de la Abogacía Española. Libro de ponencias y comunicaciones, Consejo General de la Abogacía Española, Aranzadi, Navarra, 1999, pp. 322-332.

- *Las páginas web como soporte de condiciones generales contractuales*, Premio Estanislao de Aranzadi 2002, Thomson-Aranzadi, Navarra, 2003.
- “La defensa letrada y el devenir tecnológico”, *Foro Galego*, revista del Ilustre Colegio de Abogados de A Coruña, de la Real Academia Gallega de Jurisprudencia y Legislación, y de la Universidad de A Coruña, núms. 196-197, segundo semestre 2006-primer semestre 2007, pp. 337-374.
- “Encriptación y firma electrónica”, *Internet: un nuevo horizonte para la seguridad y la defensa*, FERNÁNDEZ RODRÍGUEZ, J.J. (ed.), Universidad de Santiago de Compostela, 2010, pp. 185-205.
- “Encriptación y firma electrónica”, *Internet: un nuevo horizonte para la seguridad y la defensa*, FERNÁNDEZ RODRÍGUEZ, J.J. (ed.), Universidad de Santiago de Compostela, 2010, pp. 185-205.
- *La singularidad de la Abogacía (De entre las profesiones liberales)*, Premio Jurídico Internacional del Instituto Superior de Derecho y Economía (ISDE), Difusión Jurídica-Economist&Jurist, Madrid, 2017.
- *La relación abogado-cliente. El contrato de servicios del abogado*, Premio Memorial Degà Roda i Ventura del Colegio de Abogados de Barcelona, Colección Grandes Tratados, Aranzadi, Navarra, 2017.
- *La ciberseguridad como deber deontológico del abogado. El secreto profesional y la protección de datos*, La Ley - Wolters Kluwer, Madrid, 2019.

PARLAMENTO EUROPEO: “Las fuentes y el ámbito de aplicación del Derecho de la Unión Europea”, perteneciente a las *Fichas técnicas sobre la Unión Europea*, 2017, pp. 2-3. Disponible en: [http://www.europarl.europa.eu/ftu/pdf/es/FTU\\_1.2.1.pdf](http://www.europarl.europa.eu/ftu/pdf/es/FTU_1.2.1.pdf) (visitado en fecha 16 de octubre de 2017).

PÉREZ ANDÚJAR, C.: “REDABOGACÍA: impulsando y liderando la transformación tecnológica de la Abogacía española”, *Abogacía Española*, núm. 108, febrero 2018, p. 29.

PÉREZ BES, F.: “Lo que nos enseñan las crisis de ciberseguridad”, *Abogacía Española*, núm. 109, mayo 2018, p. 29.

REAL ACADEMIA ESPAÑOLA: *Diccionario de la Lengua Española*, 22<sup>a</sup> ed., Madrid, 2001.

RIGO VALLBONA, J.: *El secreto profesional de abogados y procuradores en España*, Bosch, Barcelona, 1988.

ZURITA CARRIÓN, J.: “El secreto profesional: razón y límites”, *Deontología y práctica de la Abogacía del siglo XXI*, MENÉNDEZ MENÉNDEZ, A., y TORRES-FERNÁNDEZ NIETO, J.J. (dirs.), Aranzadi, Navarra, 2008, pp. 49-81.