La inteligencia artificial como motor de progreso: el difícil equilibrio entre los derechos de propiedad intelectual y la privacidad (1)

Nuria Fernández Pérez
Catedrática de Derecho Mercantil
Universidad de Alicante
LA LEY mercantil, Nº 85, Sección Derecho digital / Doctrina, Noviembre 2021, Wolters Kluwer

LA LEY 12620/2021

Resumen

La innovación basada en inteligencia artificial está llamada a jugar un papel esencial en la mejora de las condiciones de la sociedad y en el crecimiento económico. Por ello debe ofrecerse una adecuada protección y seguridad jurídica a quienes invierten en estas herramientas de innovación tecnológica. No obstante, los sistemas de inteligencia artificial se nutren de un volumen ingente y muy variado de datos que son recogidos y tratados con fines diversos. Esto puede, en ocasiones, menoscabar derechos fundamentales; y, en particular, afectar a la privacidad de las personas. La necesidad de una regulación que permita compatibilizar ambos aspectos se muestra cada vez más imperiosa. Por ello, resulta de especial interés la propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas en materia de inteligencia artificial. La opción por mecanismos como la privacidad desde el diseño y la rendición de cuentas de los sistemas de inteligencia artificial y de sus resultados, tanto antes como después de su implementación pueden contribuir a mantener ese necesario equilibrio entre los derechos fundamentales y los de propiedad intelectual, aunque se antoja una tarea complicada.

Palabras clave

Inteligencia Artificial (IA), Big Data, derecho a la intimidad personal y familiar, protección de datos, propiedad intelectual, Reglamento europeo en materia de Inteligencia Artificial.

Abstract

Intelligence Artificial innovation will play an essential role in improving social conditions and economic growth. Therefore, those investing in technological innovation must be assured that their investment is properly protected. However, IA systems require a very large and varied volume of data that are collected and processed for different purposes. It can sometimes undermine fundamental rights and affect the privacy. The need for a regulation to reconcile both aspects is becoming increasingly urgent. For this reason, the proposal for a European Union Regulation laying down harmonised rules on artificial intelligence is of great interest. The option for mechanisms such as privacy by design and accountability of AI systems and their results, both before and after their implementation, can contribute to maintaining the necessary balance between fundamental rights and intellectual property rights, although it seems like a complicated task.

Keywords

Artificial Intelligence (AI), Big Data, right to privacy, data protection, intellectual property rigts, European Union Regulation on artificial intelligence.

I. La economía de los datos en el marco de la cuarta revolución industrial

1. Consideraciones generales

La economía mundial se está convirtiendo con gran rapidez en digital. De hecho, pocas épocas de nuestra historia han soportado una disociación más radical entre los avances tecnológicos y su consecuente proyección social, así como sobre los conceptos jurídicos destinados a regularlos. Uno de los ámbitos donde la transformación está siendo mayor es, sin duda, el de los datos y el de su consideración jurídica. Los datos personales, hasta el momento guardaban una estrecha relación con la intimidad de las personas, con su privacidad. A esa vertiente, se une ahora también, la relacionada con la economía de los datos, esto es; su consideración como activos económicos (2) .

Tal y como señala la Comisión Europea, «los *datos están en el centro de la transformación»* y «*son elemento vital del desarrollo económico*» (3) . La innovación basada en datos está llamada a jugar un importante papel en la mejora de las condiciones de la sociedad y en el crecimiento económico. Los datos remodelarán las formas de producir, consumir y vivir. Los beneficios se harán sentir en cada uno de los aspectos de nuestra vida, desde un consumo energético más consciente y la trazabilidad de los productos, materiales y alimentos, hasta unas vidas más sanas y una mejor atención médica (4) .

En la actualidad se genera una información realmente incuantificable y además no estructurada. Hablamos, por tanto, de datos que no pueden ser tratados en el modo convencional puesto que superan los límites y capacidades de las herramientas de *software* que se venían utilizando. Esa información, esos datos, considerados de forma aislada no tienen excesivo valor; sí desde luego, cuando se entrelazan, puesto que pueden permitir obtener información adicional, diferente a la que proporcionan los datos de forma aislada. Se necesita por ello poner en valor esos datos y de ahí, la importancia del proceso de digitalización que se extiende en todos los ámbitos, tanto en el público como en el ámbito de los negocios; y, que ha dado lugar a una auténtica revolución en el modo de capturar, procesar, analizar y visualizar los datos (5) . Se trata de la tecnología Big Data, expresión con la que se pretende hacer referencia a nuevas tecnologías que permiten analizar ágilmente, mediante el uso de complejos algoritmos, cantidades masivas de datos provenientes de fuentes dispares con la finalidad de obtener conclusiones aplicadas a los más distintos fines (6) .

Se caracteriza, por tanto, porque es una tecnología en la que se constatan —tal y como se ha popularizado— las «tres uves»: «volumen», puesto que habilita para manejar grandes cantidades de datos; «variedad», dado que el origen de esos datos puede ser muy variado; y «velocidad», en el sentido de rapidez, incluso inmediatez, para manejar los datos. A estas, se han añadido posteriormente otras, como la veracidad de los datos y la posibilidad de visualizarlos. Esta tecnología que se complementa con la relativa a la computación en la nube (*cloud*) que es utilizada de forma mayoritaria en el mundo empresarial dado que permite acceder a la información en cualquier momento, desde cualquier lugar y desde cualquier dispositivo; por lo tanto, es una herramienta que contribuye el mejor desarrollo de los negocios.

Esta revolución tecnológica no puede entenderse sino es en el marco de lo que ya se denomina la Cuarta Revolución Industrial o industria 4.0 (4IR en sus siglas en inglés) que se está difundiendo a una velocidad sin precedentes al estar impulsada precisamente por medios digitales y tecnológicos. Fenómeno que hace referencia a la introducción de las tecnologías digitales en la industria concebida en sentido amplio (7) . La

singularidad del proceso consiste en que la tecnología logra que dispositivos y sistemas colaboren entre ellos y con otros, en una suerte de hibridación entre el mundo físico y el digital, es decir, posibilitan la vinculación del mundo físico (dispositivos, materiales, productos, maquinaria e instalaciones) al digital (sistemas), lo que, a su vez, permite modificar los productos, los procesos y los modelos de negocio, con lo que ello significa de salto cualitativo en la organización y gestión de la cadena de valor de los distintos sectores (8) .

En la economía de los datos, un pilar fundamental, junto con el *Big Data*, es la inteligencia artificial (en adelante IA). Sin darnos cuenta realmente, la IA ha entrado a formar parte de nuestra vida cotidiana (9) : asistentes digitales como Google Home, Amazon Echo, asistentes como Alexa Siri, Cortana, asistentes para la conducción de vehículos autónomos; asistentes como los denominados agentes conversacionales, que son aplicaciones programadas para simular una conversación de lenguaje natural. Encontramos también la IA en el internet de las cosas (IoT), en las técnicas de marketing para segmentar a la clientela, en las soluciones de análisis de comportamiento de los consumidores para identificar los consumidores potenciales y la optimización de los productos (10) .

No existe como tal una definición de IA universalmente admitida, tras más de siete décadas desde que se produjo el primer acercamiento a la IA como disciplina (11) . Al margen de su concreta concepción, podemos considerar que la IA (*artificial intelligence*, AI) consiste, básicamente, en emular las diversas capacidades del cerebro humano para presentar comportamientos inteligentes sintetizando y automatizando tareas intelectuales, a través de determinadas secuencias de instrucciones —estructura algorítmica— que especifican las diferentes acciones que debe ejecutar el computador para resolver un determinado problema (12) . En la Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones-IA para Europa de 25 de abril de 2018 se considera que es un término que se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos (13) . En el proyecto de futuro Reglamento europeo sobre IA (14) , en lugar de ofrecer una definición concreta se opta por considerar que se trata de una familia de tecnologías en rápida evolución (15) . En esa tecnología podemos encontrar tanto *software*, es el caso de los asistentes virtuales, *software* de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento de voz y rostro; como IA integrada, esto es, robots, drones, vehículos autónomos, y la tecnología IoT (Internet de las Cosas). El objetivo es potenciar la capacidad tecnológica e industrial de la UE, a través del impulso y la adopción de la IA en todos los ámbitos de la economía, tanto en el sector privado como en el público (16) , y se reconoce que la IA puede contribuir de modo significativo a mejorar los servicios públicos en la Unión Europea (17) .

En definitiva, de lo que se trata es de una traslación al Derecho de un fenómeno ya presente en nuestros días y que va a caracterizar tiempos no muy lejanos, como es la progresiva sustitución del hombre por máquinas, con el matiz, de que se trata de máquinas cada vez con mayor capacidad y más inteligentes, en el sentido de poder actuar con autonomía. Es decir, que los programas informáticos y las máquinas pueden realizar de forma más eficiente tareas realizadas hasta ahora por las personas, lo que supone un cambio estructural en el sector productivo y en el mercado de trabajo. Ya se habla de que nos encontramos en la «*Artificial Invention Age*» (18) , en la que la colaboración entre las personas y las máquinas, se convierte en un punto nuclear, en la que los humanos son los encargados de detectar el problema y concretarlo, y las máquinas las que tienen que generar, simular y evaluar las posibles soluciones. Pero, para que ello sea posible, precisan de datos. Es en el modo de obtención de los datos, cómo y para qué usos se recopilan, y cómo se tratan y utilizan donde entra en juego otro aspecto que resulta esencial, como es la necesidad de garantizar que con estos desarrollos no se vulneren las libertades y derechos fundamentales, en particular, y por lo que a este trabajo respecta, los derechos a la intimidad y a la protección de datos.

2. El eventual conflicto entre la protección de la propiedad intelectual y los derechos a la protección de los datos personales y la intimidad: enunciado y remisión

Para la Unión Europea constituye una prioridad avanzar en la construcción de un Mercado Único Digital en el que la libre circulación de mercancías, personas, servicios y capitales esté garantizada y en el que personas y empresas pueden acceder fácilmente a las actividades y ejercerlas en línea en condiciones de competencia, con un alto nivel de protección de los datos personales y de los consumidores, con independencia de su nacionalidad o lugar de residencia (19) .

El tratamiento de los datos, y la IA en sus diferentes manifestaciones plantea más que nunca la existencia de un conflicto entre información y privacidad; entre protección de datos y desarrollo empresarial (20) .En efecto, si muchas de las innovaciones que sustentan la transformación digital se basan en nuevas herramientas y aplicaciones sustentadas en IA, resulta clave y una de las primeras cuestiones a considerar, analizar cuáles los mecanismos jurídicos que van a permitir proteger esa innovación. Sin seguridad jurídica para quienes invierten mucho dinero en nuevos desarrollos de IA no habrá inversión. Sin inversión no habrá innovación. Y sin innovación, lógicamente, no habrá progreso ni crecimiento. Se trata de determinar qué tipos de innovaciones pueden ser patentadas y si hay otros métodos de protección jurídica alternativos o compatibles. Pero no solo los sistemas de IA constituyen una pieza central para el desarrollo. Los datos, en sí mismo considerados, son una fuente de riqueza para las empresas, y como tal, su objetivo va a ser conseguir su protección, siendo una de las vías, las del secreto empresarial.

No obstante lo anterior, si la fuente son los datos, resulta esencial determinar cómo se obtienen esos datos y cómo se tratan. Encontramos aquí, por un lado, aspectos relativos a la protección que el ordenamiento jurídico dispensa a la protección de los derechos a la intimidad personal y familiar y a la protección de datos, tomando el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales como su principal referencia. Pero simultáneamente, debe ponerse en conexión con el propio contenido del derecho de patente, si es el caso, o del derecho de autor, o de otros derechos conexos, o la protección que brinda el secreto empresarial.

En particular, el derecho de patente, se configura como un derecho negativo o de prohibición, en el sentido de excluye el empleo por terceros de la regla técnica reivindicativa de la patente (21) . Esto plantea un problema cuando se trata de decisiones basadas en datos provenientes de sistemas automatizados que parten de IA, y en los que se pueden producir tratos discriminatorios utilizando datos que vulneran la intimidad personal y familiar y la protección de los datos de las personas. También los derechos de autor tienen una vertiente negativa, consistente en prohibir la realización de cualquier acto de explotación a todo tercero, sin su autorización. Aspectos que se abordarán con posterioridad.

Finalmente, no hay que olvidar, la existencia de un problema general derivado del modo radicalmente distinto en el que se protegen los datos personales en el ámbito de la Unión Europea y en Estados Unidos. En la Unión Europea gozamos de un marco legal garantista, caracterizado por su carácter reglado, y en el que se consideran ambos derechos como fundamentales. En Estados Unidos no se dispone de una legislación federal. Únicamente en algún estado como California, se cuenta con una norma al respecto (22) . Es cierto que esta situación puede cambiar, puesto que se está promoviendo una normativa federal, si bien ya hay voces críticas respecto a las mismas, al estar liderada por las grandes empresas tecnológicas. En todo caso, los datos se conciben como un bien patrimonial, cuya protección, salvo lo contenido en alguna ley especial, corresponde al propio individuo (23) .

II. Los datos y la innovación basada en IA : la evolución de los derechos a la intimidad personal y familiar y a la protección de datos

1. Incidencia del contexto tecnológico en los derechos a la intimidad personal y familiar y a la protección de datos de carácter personal

En este contexto de revolución tecnológica y apoyándose en numerosas ocasiones en la tecnología que proporciona la IA, las empresas logran obtener una inmensa cantidad de datos. Resulta cada vez más habitual la difusión por parte de las personas físicas de un importante volumen de datos personales. En la actualidad, las grandes compañías tecnológicas que dominan el mercado, las denominadas GAFA (Google, Apple, Facebook y Amazon) a la que habría que añadir también Microsoft, así como las de origen asiático las denominadas BAXT (Baidu, Alibaba, Xiaomi y Tecent) tienen acceso a un número muy elevado de datos de sus clientes. Datos que obtienen tanto por sus relaciones directas con los mismos, como de empresas relacionadas con ellas que prestan servicios como titulares de redes sociales, buscadores o servicios de compra muy extendidos en la actualidad. La aplicación de programas de IA y el manejo de los datos resultantes, permiten a estas empresas crear auténticos perfiles digitales de sus clientes. Ello les permite, lógicamente, afinar mucho en sus políticas de venta y publicidad perfectamente adaptadas a los gustos y preferencias de sus clientes. También les permiten conocer las tendencias del mercado y prepararse adelantándose a cualquier competidor o entrando en nuevos mercados (24) .

Una de las cuestiones que se plantean es que los datos son proporcionados en ocasiones de forma consciente, pero en otras muchas de forma inconsciente. En efecto, cada vez en mayor medida hay productos de consumo impulsados por la IA equipados con frecuencia con sensores que generan y recopilan grandes cantidades de datos sin el conocimiento o consentimiento de quienes se encuentran en su proximidad con el peligro de que esos datos son tratados para obtener informaciones diversas. Son muchos los datos que generamos sin saberlo teniendo en cuenta que cada vez más, vivimos vinculados con dispositivos inteligentes (teléfonos, tarjetas, gps, relojes,etc), etc. Estos dispositivos producen millones de datos que, aunque en principio puede pensarse que son anonimizados, son uno de los bienes más valiosos en la actualidad y desde luego en el futuro inmediato (25) . Buena prueba de ello es la gratuidad de las redes sociales que en realidad se cobran con la propaganda, incluso personalizada que reciben los usuarios, y con la venta de sus datos a terceros (26) .

La IA se puede utilizar para inferir hechos sensibles a partir de datos relativamente mundanos, aprendiendo sobre los estados emocionales, la salud, la política y otros de las personas a partir de datos como el historial de ubicaciones e interacciones en las redes sociales. La protección del derecho a la privacidad es clave para el disfrute de una serie de derechos conexos, como la libertad de expresión, asociación, política participación e información

La globalización y el desarrollo tecnológico, por tanto, plantean nuevos retos para la protección de los derechos fundamentales. Desde la Unión Europea (27) , es claro el compromiso acerca de que el ser humano es debe seguir siendo lo más importante, lo que implica que habrá que aprovechar la oportunidad que brindan los datos que sirven de fuente para entrenar a los sistemas de IA, y establecer las medidas para que se garantice un acceso mejor a los datos y un uso responsable de los mismos (28) .

Son múltiples las cuestiones que surgen en torno a los datos: cómo se accede a los datos, y quién es el usuario de los datos, y en qué condiciones puede intercambiarse información entre el sector público y las empresas o entre las empresas entre sí. El *Big Data* y su tratamiento supone un salto cualitativo muy importante que coloca a quien dispone de los datos y del conocimiento y técnicas para tratarlos en una situación de ventaja competitiva sin precedentes (29) , que puede distorsionar la libre competencia que constituye un pilar para el correcto funcionamiento de los mercados y también para la protección de cuantos intervienen en los mismos, tanto empresas competidoras, como los ciudadanos (30) .

También, no debe obviarse la posible inclusión de sesgos (por ejemplo, a la hora de determinar cómo está escrito el código de programación del algoritmo), tanto involuntarios como voluntarios (31) . En ambos casos, y derivada de la llamada «vigilancia algorítimica» (32) . se puede llegar a decisiones perjudiciales (33) . para los destinatarios de las decisiones que se tomen en base a los mismos, y además, en el caso de que fueran voluntarios, pueden provocar suponer actuaciones de competencia desleal.

Uno de los rasgos de la sociedad digital es que se amplía la fuente posible de riesgos para las libertades, puesto que no tienen su origen solo, de forma mayoritaria de los poderes públicos, sino también de las empresas y otros ciudadanos. En todo caso, y sin ser posible ahondar en cada una de esas cuestiones, lo que resulta claro es que resulta preciso contar con un marco jurídico adecuado para dar respuesta a los retos que se plantean en un nuevo contexto de negocios en un mundo digital, y, en particular, cuando lo que se utilizan son datos de personas, atender de forma preferente a la protección de los derechos fundamentales de la ciudadanía. A través de algoritmos alimentados con datos obtenidos de fuentes muy diversas, se puede realizar una previsión sobre las conductas futuras de una persona, de modo que la persona pueda ser evaluada por esas predicciones y no realmente por sus acciones.

Los «nativos digitales» crecen con la aceptación de la pérdida del anonimato y de la intimidad, cuestiones que sin embargo se vinculan a los propios derechos fundamentales que reconoce la Constitución. Es por ello que la aplicación de los derechos fundamentales a la propiedad intelectual (34) y a las normas en materia de protección de datos pueden conducir a recobrar la «verdadera función» de los derechos, en cuanto pueden usarse para servir de equilibrio entre la protección que confieren y los excesos de sus titulares (35) . Tal y como ha señalado la Comisión Europea, en una sociedad en la que la cantidad de datos que se generan es cada vez mayor, resulta esencial determinar la forma en la que se recogen y utilizan esos datos, que debe «*situar los intereses de la persona en primer lugar, de conformidad con los valores, los derechos fundamentales y las normal europeas*» (36) . Con estas premisas, el uso de la tecnología puede contribuir, sin duda, a potenciar la innovación y el crecimiento.

Otro aspecto clave relacionado con el uso de algoritmos para el procesamiento automatizado de datos se centra en el almacenamiento de datos en la «nube» (*cloud*). Con ello, los archivos y otros datos ya no se guardan en un almacenamiento local, sino que se almacenan de forma remota en servidores accesibles a través de Internet. El problema es que los datos de los usuarios pueden ser procesados por algoritmos mientras se almacenan remotamente de formas intrusivas. Dicho procesamiento automatizado de datos puede tener lugar en dos lugares: bien en tránsito a la ubicación de almacenamiento de red remoto; o, bien en los servidores remotos donde los datos se almacenan. Puede resultar cada vez más difícil para los usuarios determinar si están utilizando servicios locales o remotos, y si ello tiene consecuencias en la esfera de sus derechos (37) .

2. La evolución del derecho a la intimidad personal y familiar en la era digital

Con bastante frecuencia, la protección de datos de carácter personal se confunde con el respeto al derecho a la intimidad. Sin embargo, tienen orígenes y perímetros de actuación diferentes (38) .

La heterogeneidad en los intentos para conceptuar el derecho a la intimidad es muy amplia. Por la complejidad del término y su variabilidad según criterios sociales de un lugar o de una época determinada, la definición de este derecho, la fijación de su contenido y límites no está exenta de problemas. Hay que tener en cuenta que para ello se requiere delimitar conceptos de difícil precisión, tales como vida privada, círculo íntimo, esfera reservada a la persona, etc. El concepto de la intimidad es bastante impreciso y tiene múltiples facetas (39) . También, tiene una muy diferente concepción en el ámbito europeo y el estadounidense (40) . Mientras que en Europa se vincula con la dignidad de la persona, que se ve amenazada por los medios de masas, en Estados Unidos, se piensa en la libertad, siendo su principal amenaza el gobierno. Por otra parte, la diferencia es clara en orden a su reconocimiento en textos legislativos. Mientras que en Estados Unidos esto apenas se produce, en el continente europeo no solo está recogido en leyes (como en el artículo 7º de la Carta de los derechos fundamentales de la Unión Europea (41)), sino que además suele tener reconocimiento constitucional, como sucede con nuestro país.

El derecho a la intimidad es un derecho consagrado en la Constitución española (42) , en su artículo 18.1, de Título I (De los derechos y deberes fundamentales), donde se establece que: «*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*». Son tres, por tanto, los derechos que forman el denominado bloque de derechos de la personalidad (43) : la intimidad, la propia imagen y el honor. Se trata pues de un derecho personalísimo y ligado a la misma existencia del individuo (44) .

En el artículo 18.1 CE no se ofrece ninguna definición de derecho a la intimidad, y han sido muchas en este sentido las aportaciones doctrinales dirigidas a ofrecer un concepto. El Tribunal Constitucional se ha mostrado partidario de construir ese concepto teniendo especialmente en cuenta el aspecto subjetivo de la intimidad, entendido como el derecho a no ser conocidos, en algunos aspectos concretos, por los demás (45) .Se trata de garantizar al individuo un ámbito reservado de su vida frente a la acción y el conocimiento de terceros. Este ámbito se protege tanto respecto de los poderes públicos como de los particulares, y se encuentra vinculado de manera inmediata y directa con el respecto de su dignidad como persona, su personalidad, siendo necesario para mantener su calidad mínima de vida humana. Como señaló el Tribunal Constitucional en su Sentencia 20/1992, de 14 de febrero, sin este derecho no sería realizable, ni concebible la existencia de la dignidad que a todos quiere asegurar la norma fundamental.

Se trata, como también ha señalado el Tribunal Constitucional, de un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio (46) .

Frente a la concepción originaria de ese derecho vinculado a la propia personalidad, a la dignidad, en su última jurisprudencia el Alto Tribunal reconoce que el derecho a la intimidad incluye temas muy sensibles y cada vez más variables, alcanzando temas como el cuerpo, la salud, el sexo, la vida familiar y otros ámbitos.

Por otra parte, si ya es difícil conceptuar que se entiende por intimidad, más lo es delimitar qué es intimidad personal y familiar. Es algo variable, dependiendo del tiempo concreto y la sociedad. Respecto a la intimidad familiar, el Tribunal Constitucional ha indicado en su Sentencia 231/1988, de 2.12.1988 (Fundamento Jurídico Cuarto), que son «(…) *determinados aspectos de la vida con otras personas, con las que guarda una especial y estrecha vinculación, como es la familiar, aspectos que, por la relación o vínculo existente con ellas, incide en la propia esfera de la personalidad del individuo*».

Las personas pueden decidir libremente revelar datos relativos a su persona y también a quién se los van a revelar. Con ello, no se renuncia al derecho a la intimidad. Forma parte del contenido de los derechos, decidir cómo se ejercen y por tanto, puede considerarse que permitir de forma voluntaria una «intromisión» en la esfera personal y familiar es una forma de ejercer el derecho. La clave se encuentra en que el sujeto haya prestado su consentimiento expreso o tácito al acceso a la información (47) . En definitiva, ejercer el derecho a la intimidad es consentir o no que un tercero acceda a lo que cada cual tiene por íntimo (48) . El Tribunal Constitucional en su STC 173/2011, de 7 de noviembre de 2011 con mucha claridad establece que *«(…) no obstante lo anterior, hemos afirmado que el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29.06.2009)»* Fundamento Jurídico Tercero).

El Tribunal Constitucional deja igualmente claro que el derecho a la intimidad se vulnerará cuando la intromisión en el ámbito íntimo y familiar del sujeto, aun cuando hay sido consentida *«subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida* (49) *».* En esta línea, también resulta muy gráfico el Alto Tribunal cuando indica que en los casos en los que se revela una información personal a través de un *medio virtual de comunicación prestado por la red, el titular del derecho fundamental a la intimidad «está tolerando la intromisión en su «intimidad», el acceso de otra persona a su esfera privada y el uso de la información así adquirida».*

En cualquier caso, el hecho de permitir el acceso al círculo íntimo de la persona no significa que se pierda todo el control sobre la información (50) . Entra aquí en juego el derecho a la protección de datos, como derecho autónomo, que confiere al sujeto que ha autorizado el acceso a su intimidad el derecho a seguir manteniendo un poder de control sobre el uso y destino de esa información.

Al margen de que pueda defenderse la sustantividad del derecho de protección de datos, lo cierto es que el derecho a la intimidad está especialmente amenazado ante el desarrollo de la tecnología. Internet no representa por sí mismo una amenaza por el hecho de que tenga un carácter abierto. El aspecto importante es que existen tecnologías sustentadas en sistemas de IA capaces de monitorizar el comportamiento de los usuarios de internet, convirtiendo en banal su consentimiento.

3. El derecho a la protección de datos

Tal y como se acaba de indicar, el derecho a la protección de datos es un derecho dotado de sustantividad propia, si bien su reconocimiento se produce con posterioridad al del derecho a la intimidad.

En el ámbito internacional, el derecho de protección de datos se recoge por vez primera en el Convenio para la protección de las personas físicas en relación con el tratamiento automatizado de datos personales (Convenio 108). En este convenio, se alude en su artículo 2.a a los «datos de carácter personal» como aquellos que vienen referidos a cualquier información relativa a una persona física identificada o identificable. No se trata, por tanto, solo de los datos que pueden estar vinculados a la esfera personal y familiar, sino a cualesquiera datos.

En el ámbito de la Unión Europea, en la Directiva 95/46 CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se alude que los sistemas de tratamiento de datos deben respetar las libertades y derechos fundamentales de las personas físicas, y entre ellos, en particular, la intimidad (considerando segundo). Por su parte, la Carta de Derechos fundamentales de la Unión Europea, contempla en su artículo 8º la

protección de datos de carácter personal como derecho fundamental (51) .

En nuestro país, podemos hablar de una evolución semejante. En la Constitución no se diferencia de forma clara entre el derecho a la intimidad y el de protección de datos, aun cuando en el artículo 18.4 se alude, como ya hemos tenido ocasión de señalar que « *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*».

Ya en la Ley orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD), se aludía a la diferencia entre intimidad y privacidad (52) . Y, en la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales se recoge ya como derecho fundamental autónomo enmarcado en el artículo 18.4 CE.

Sin duda, en nuestro país, frente a la jurisprudencia más vacilante del Tribunal de Derechos Humanos y del Tribunal de Justicia de la Unión Europea (53) , es la jurisprudencia constitucional la que más ha contribuido a afirmar la sustantividad del derecho de protección de datos. Tal y como se ha señalado, se ha producido una evolución desde la idea recogida con carácter inicial en la Constitución en la que aparece un mandato al legislador a una construcción jurisprudencial acerca de la existencia de un nuevo derecho fundamental, autónomo e independiente de los demás (54) . Es el Tribunal Constitucional el que establece en su famosa Sentencia 94/1988, que el artículo 18.4 consagra «*un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona*» (55) . Y de manera más contundente, en las Sentencias 290/2000 de 30 de noviembre de 2000 y Sentencia 292/2000, de la misma fecha, en la que el Alto Tribunal habla de la «*singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respecto a la dignidad personal …..el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal».*

En definitiva, se trata de un poder de disposición y de control sobre los datos personales que «*faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, así como saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso* (56) , salvo que exista habilitación legal para que los datos puedan ser tratados sin dicho consentimiento» (57) . Su finalidad es impedir el tráfico ilícito y lesivo de esos datos para la dignidad y los derechos del afectado.

Junto a esta parcela de contenido, el derecho fundamental a la protección de datos también se diferencia del derecho a la intimidad personal y familiar en que otorga a la persona el poder obligar a terceros a abstenerse de la utilización de los datos, esto es, otorga el poder de control sobre los datos personales (entre los cuales también están, lógicamente los relacionados con la esfera íntima de la persona) (58) .También desde la doctrina constitucionalista se ha incidido en la idea que «el bien jurídico» al que se refiere el artículo 18.4 CE no solo viene referido a la reserva personal y familiar, sino también «*a los derechos, libertades y garantías fundamentales de los ciudadanos*», siendo muchos los matices que se aporta en torno a la diferenciación de ambos derechos (59) .

4. Hacia la construcción de nuevos derechos vinculados al mundo digital

Tal y como se ha señalado con anterioridad, los derechos a la intimidad personal y familiar y a la protección de datos son derechos autónomos, si bien con evidentes nexos de unión en el contexto del mundo digital (60) . La irrupción de la tecnología ha transformado nuestra vida (61) . La revolución tecnológica se plantea como «reto ineludible» para el análisis de los derechos humanos, que resultan afectados «*en su significación, fundamento y en su realización y garantía*» por unos desarrollos tecnológicos que cuestionan valores como la dignidad, la libertad, la autonomía, la identidad y la igualdad, que constituyen el centro de gravedad en torno al cual se construye el sistema de derechos y libertades (62) .

La categoría de los derechos humanos no constituye un concepto invariable, sino que se haya sujeta a cambio atendiendo a cada época concreta; y, ha sido particularmente afectada por los desarrollos técnico-científicos. Por ello se alude a los derechos humanos como categorías históricas. También ha tenido su reflejo en los derechos y libertades de la ciudadanía, impactando de un doble modo: por una parte, con el nacimiento de nuevos derechos, y por otra, por su repercusión en algunos de los ya existentes. Esto es algo que no se discute.

La cuestión que divide a los constitucionalistas, es si en esa evolución que sufren los derechos fundamentales, nos encontramos en una tercera generación de derechos (63) o en una cuarta generación (64) . En cualquiera de los casos, el derecho a la protección de datos se incardina en los derechos de última generación

Cabe en este sentido mencionar la llamada Carta de Derechos Digitales (65) , que se enmarca dentro de la «Agenda España Digital 2025». No se trata de un texto con carácter normativo; por tanto, no puede entenderse sino es dentro del marco legal existente. Su objetivo es servir como referencia en la actuación tanto de los poderes públicos, como de los particulares. En la Carta se recogen seis categorías de derechos (66) , entre los que se encuentran algunos ya consagrados legalmente, como es el caso del derecho de protección de datos; y otros, que suponen una adaptación de derechos existentes al nuevo escenario digital. Así, se alude a los derechos ante la inteligencia artificial, tomando como objetivo lograr una IA centrada en la persona. Por ello, se parte del reconocimiento de la no discriminación algorítmica o el derecho de la persona a solicitar una supervisión o intervención humana.

En todo caso, y volviendo al plano legal, diferenciar el derecho a la intimidad y el de protección de datos, no está del todo resuelto ni en el derecho español, ni tampoco en el comparado. La normativa en materia de protección de datos personales distingue un núcleo duro de datos «sensibles» o «especialmente protegidos» que son los que coinciden con la esfera de intimidad especialmente protegida (67) . El TJUE en una numerosa jurisprudencia ha contribuido a delimitar el contenido del concepto dato personal, a partir de la definición contenida primero en la Directiva y posteriormente en el Reglamento (68) y que difieren escasamente. De este modo, ha incluido el apellido y el nombre, las huellas dactilares, la imagen, datos fiscales (69) .

La protección que otorga el derecho a la intimidad no se extiende a toda la información sobre la persona, sino solo la relativa a determinados aspectos de su vida; aquellos que tienen la consideración de íntimos, y tampoco implica facultades positivas, es decir, el derecho a obtener prestaciones de terceros; sino que se limita a una vertiente negativa, que consiste en la facultad del titular del derecho de imponer a los terceros una abstención de intromisión o injerencia en aquella parcela protegida por el derecho. No obstante, «garantizar la vida privada, hoy, precisa del reconocimiento del individuo de un poder de control sobre todos sus datos personales». Transparencia vs. protección de datos (70)

Así, en la actualidad, se habla de la construcción de un derecho fundamental al propio entorno virtual (71) en el que quedarían englobados derechos diferentes que pueden —y suelen, además— encuadrarse dentro del artículo 18.1 CE —entraría aquí la protección del listado de contactos o de fotografías—; el derecho al secreto de las comunicaciones recogido en el artículo 18.3 CE —se pone como ejemplo la garantía de

las comunicaciones a través de sistemas de mensajería—; o el propio derecho a la protección de datos del artículo 18.4 CE —en relación, por ejemplo, con los datos de geolocalización—.,

Ambos derechos pueden encuadrarse dentro del paraguas amplio de la privacidad, dentro del cual podrían englobarse conceptos como el de intimidad, protección de datos, confidencialidad e incluso identidad digital (72) . La privacidad contempla un ámbito por tanto, más amplio; mientras que con el derecho a la intimidad se protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. La jurisprudencia viene ya marcando las pautas para poder limitar ese derecho al propio entorno virtual, en la medida en que se exige una autorización jurisdiccional que habilite el «sacrificio» de derechos como el de intimidad o secreto de las comunicaciones (73) .

III. Algoritmos y técnicas de procesamiento automático de datos: impacto en los derechos fundamentales y en los derechos de propiedad intelectual

1. El conflicto entre derechos: aspectos técnicos y jurídicos

a) Planteamiento

La IA y Big Data son dos herramientas tecnológicas que tienen una especial interrelación. A través de algoritmos, se puede realizar una previsión sobre las conductas futuras de una persona, de modo que la persona pueda ser evaluada por esas predicciones y no realmente por sus acciones. Como se ha ya señalado, los desarrollos en materia de IA necesitan una estructura de datos de la que poder disponer y que resulte fiable. La evolución de la IA precisa un gran volumen de datos para que pueda llevarse a cabo el *training* de los sistemas. Por tanto, cuanta mayor cantidad de datos, mayor es la potencialidad del sistema para poder aplicar, en base al conocimiento de los datos que ya contiene el sistema, respuestas ante nuevos datos (74) . Y, de forma paralela, el tratamiento de los datos requiere de una computación de alto rendimiento (75) . las nuevas tecnologías de computación, almacenamiento y comunicación, y la IA deben entrelazarse cada vez más para que esta última consiga sus objetivos.

Los algoritmos juegan por tanto un papel esencial en la toma de decisiones, bien aportando información a quien tiene que decidir, bien prediciendo decisiones, o bien guiando la elección. Siendo cierto, como ya se ha destacado, que se trata de un recurso eficaz, y rápido para tratar volúmenes de datos inaccesibles para los humanos, también lo es que su generalización puede poner en tela de juicio los derechos de los individuos que son desprovistos de su facultad de iniciativa y de la autonomía que les resulta propia, partiendo de la elaboración de perfiles con una suma de datos sobre los que no se tiene control (76) .

Se ha señalado en este sentido, que los algoritmos no siempre son fiables, pueden tener efectos discriminatorios y además, en muchas ocasiones, son opacos. En primer lugar, la fiabilidad de los algoritmos depende de las fuentes de datos obtenidas. Para obtener resultados pertinentes deberían manejar un volumen de información sobre una persona importante y correctamente seleccionado. Datos que se toman desde fuentes diversas y para otras finalidades en muchos casos. Los algoritmos se registran mediante cookies y tecnologías similares como la toma de huellas digitales y datos de comportamiento generados por sensores, motores de búsqueda y asistentes virtuales. También se toman datos desde los *Smart* dispositivos, como la ubicación. Un desafío del procesamiento algorítmico de datos personales es la generación de nuevos datos (77) . Cuando se comparten datos a través de la red, es posible que esos datos puedan fusionarse, creando «una segunda e incluso una tercera generación de datos» sobre el individuo (78) .

En segundo término, es posible a la hora de inyectar los datos en el sistema, introducir determinados sesgos que lleven a que el programa ofrezca resultados también orientados, en lo que se conoce como la «discriminación algorítmica».

Y finalmente, la opacidad, el efecto o «*black box*» o «*boite noire*». Cómo podemos saber por qué un algoritmo, especialmente usando *machine learnig* ofrece una respuesta concreta. Cómo podemos conocer si se ha efectuado una combinación correcta de los datos, o incluso si estos han sido correctamente clasificados por el sistema.

Estas preguntas tienen complicada solución por dos razones: unas de carácter técnico y otras de corte jurídico. Las primeras, vienen referidas al propio sistema de funcionamiento de la técnica de IA, que hace casi imposible —por el momento— poder interpretar el resultado a la luz de los datos introducidos, en la medida que los algoritmos son sistemas para detectar correlaciones, no medios para explicar las eventuales relaciones causales existentes entre los diferentes parámetros. (79) . Cierto es, que en algunos casos muy limitados los datos puedes interpretarse.

b) Aspectos técnicos

Son muchas y variadas las formas de clasificar la IA. Algunas gozan de mayor consenso, como la que distingue entre (80) : la IA *narrow que* es la que puede desarrollar tareas predefinidas (81) ; la *general IA* (IAGI) también conocida como IA fuerte o IA profunda, que puede realizar tareas intelectuales similares a las del ser humano e incluso exceder a la inteligencia humana; y la super IA (SIA, que podría en un futuro superar de manera importante a la mente humana. También, se habla a grandes rasgos, de dos únicas modalidades, la que denomina débil, que engloba aquellos procesos que intentan simular un comportamiento humano inteligente; y la IA fuerte, que persigue pensar de manera inteligente y que será la que acerque de forma definitiva la IA a las habilidades cognitivas del ser humano y lo haga además de forma generalizada. La mayoría de las aplicaciones creadas hasta el momento pueden clasificarse como débiles, puesto que pueden tomar decisiones y resolver problemas en áreas muy específicas (es el caso de las más extendidas CORTANA, Alexa, Siri, Google Translate, etc). Sin embargo, se está avanzando de una forma vertiginosa, y hay ejemplos de IA fuerte, que plantean problemas de importante calado jurídico, que tienen que ver con el reconocimiento de derechos de propiedad intelectual al sistema de IA.

Por otra parte, la IA comprende un conjunto amplio de tecnologías, métodos y algoritmos, que permiten hablar de diversos enfoques: Sistemas que piensan como humanos (enfoque cognitivo), los que «actúan como humanos» (enfoque de la prueba de Turing); los sistemas que piensan racionalmente (enfoque de las leyes del pensamiento); y los que «actúan racionalmente» (enfoque del agente racional). Las posibilidades que ofrecen estos sistemas son muy variadas. Resulta interesante conocer su funcionamiento por cuanto se plantean problemas de carácter jurídico relacionados con las decisiones automatizadas sobre la base de estas tecnologías, y también sobre la titularidad de las creaciones realizadas por estos sistemas.

Los sistemas que piensan como humanos, son estructuras lógicas que emulan redes neuronales. Su principal característica es la «*capacidad de aprender del entorno en el que opera y mejorar su funcionamiento*» (82) . Uno de los sistemas es la denominada *Creativiy Machine*, compuesta

por redes neurales que deben ser entrenadas, que son capaces de aprender y que cuentan con una regla de aprendizaje. El hecho de que el sistema pueda realizar «creaciones» llevó a que se planteara por vez primera la preocupación acerca de la titularidad de la producción del sistema, sea en forma de invenciones o como en el caso particular, en relación con una composición musical (83) . Otro sistema, que además ha tenido y tiene un importante recorrido es el basado en algoritmos de aprendizaje automático, como la denominada *Machine Learning* (ML), en virtud de la cual, un programa de ordenador, una vez creado, y con el suficiente entrenamiento "training", es capaz de solucionar problemas distintos a aquellos para los que fue diseñado. De modo que los algoritmos inteligentes no se programan solo para resolver problemas específicos, sino también para aprender cómo resolver problemas (84) . Estos sistemas se dirigen a reproducir a través de un proceso artificial dos actuaciones propias de los humanos: de un lado, la capacidad de aprender, y de otra, el llamado aprendizaje adaptativo. Este sistema es la base de aplicaciones muy extendidas y populares, como motores de búsqueda, y filtros de spam. Son sistemas entrenados para un propósito concreto (por tanto, se encuadran dentro de la IA *narrow*) para el cual pueden lograr resultados excelentes) (85) . Como evolución del *Machine Learning* encontramos el conocido como *Deep Learnig* (DL), es una evolución del anterior, y permite emular al cerebro humano sin que haya una intervención humana previa. Se trata de redes neuronales que son un conjunto de algoritmos de aprendizaje automático —redes neuronales— inspirados en las conexiones que se producen en las neuronas del cerebro humano (86) . En este sistema, el algoritmo aprende a clasificar directamente a partir de texto, imágenes o sonido. Este sistema realiza un «aprendizaje completo», puesto que al sistema se le proporcionan datos sin procesar y una tarea a realizar, por ejemplo, clasificar la información, y aprende como hacerlo de forma automática, mejorando constantemente en la medida que se le proporcionan más datos (87)

En segundo término, encontramos el conjunto de sistemas que piensan racionalmente (enfoque racional). Se basa en un «sistema experto basado en conocimiento», que se define como un programa de ordenador que contiene la erudición de un especialista humano versado en un determinado campo de aplicación (88) .

Otro de las categorías es la de sistemas que actúan como humanos, en la que encontramos la robótica. Existe consenso en que su principal característica es la existencia de un objeto «corpóreo» que puede interactuar físicamente (89) y que puede por ello producir cambios en los objetos que hay a su alrededor (90) .

Finalmente, encontramos los sistemas que parten de un agente racional o inteligente, entendido como «*algo que razona y se encuentra dotado de controles autónomos que perciben su entorno, que persiste durante un período de tiempo prolongado, se adapta a los cambios y es capaz de alcanzar objetivos diferentes*» (91) . En los casos de robots y de sistemas inteligentes, como veremos, es donde la cuestión relativa a la titularidad de la creación resulta especialmente intensa.

c) Aspectos jurídicos

El aumento de la inversión, de la investigación y el desarrollo en estas nuevas tecnologías y en particular de la IA, ha abierto un abanico de posibilidades que afecta a múltiples áreas del quehacer humano, incluyendo el campo de la propiedad intelectual, en particular los derechos de patente (92) . En el momento actual resulta cada vez más notable el número de patentes que se registran relacionadas con la digitalización de la economía y de las propias relaciones sociales. Este tipo de invenciones se producen básicamente en los últimos diez años y el ritmo de crecimiento aumenta exponencialmente en los últimos. A efectos sistemáticos, puede hablarse de tres grupos de patentes, en cada uno de los cuales como es lógico habrá diferentes tipos de invenciones y se desarrollarán en diferentes sectores: un grupo lo constituyen las patentes en materia de hardware, *software* y conectividad, que permiten transformar cualquier objeto en un dispositivo inteligente conectado a través de internet (son la base del denominado Internet de las cosas, IoT); otro grupo es el referido a invenciones relacionadas con la seguridad, análisis de datos, IA, sistemas 3D, interfaces de usuario), que se usan en combinación con objetos; y, finalmente, un grupo amplio de invenciones más generales relacionados con procesos de fabricación, infraestructuras (vgr. ciudades inteligentes), transportes (vgr. los coches autónomos) y también con las personas (vgr. monitorización de enfermedades), por citar solo algunas de las aplicaciones más destacadas.

Este nuevo tipo de invenciones plantean interrogantes de cara su patentabilidad. Tal y como se ha señalado (93) , conforme a su configuración, la patentabilidad de la IA debe contemplarse desde dos puntos de vista: de un lado, en el de los métodos matemáticos; de otro, en el de las llamadas invenciones implementadas en ordenador. Estas últimas implican de forma necesaria un programa de ordenador para que alguna de sus funciones pueda llevarse a cabo de forma total o parcial (94) . En atención a ello se enfrenta a varios obstáculos, entre los que destaca el relativo a la eventual ausencia de carácter técnico, lo que la excluiría directamente del concepto de invención y, por tanto, de la patentabilidad (95) .

Como es sabido, los programas de ordenador y otras invenciones que tienen como base aspectos relacionados con la computación, se tratan de manera diferente por las oficinas de patentes en diferentes países. En Europa, el artículo 52 del Convenio Europeo de Patentes (CPE) excluye los programas de ordenador «como tales» de la protección de la patente. Nuestra Ley de Patentes (en adelante LP) considera no patentables los programas de ordenadores o las formas de presentar informaciones [art. 4.4 a), b), c) y d) LP], debido, según los casos, bien a su naturaleza abstracta, bien a la ausencia de carácter técnico. Ahora bien, la presencia de alguna o algunas de las materias o actividades anteriores solamente excluye la patentabilidad en la medida en que la solicitud de patente o la patente se refiera exclusivamente a ellas, no cuando se presenten junto con verdaderas invenciones (art. 4.5 LP).

La patentabilidad, por tanto, de estas invenciones o patentes (4IR) requiere un examen más preciso y si cabe especializado del estado de la técnica. A lo largo de los años, la Oficina Europea de Patentes (EPO) ha ido aclarando el art. 52 LP, determinando que es preciso un «efecto técnico», como puede ser por ejemplo que bajo la influencia del programa informático se logre el control de la ejecución del programa. De este modo, la EPO está concediendo patentes en muchos campos en los que el programa de ordenador realiza esa función técnica; también la OEPM (Oficina Española de Patentes y Marcas). Ejemplos los tenemos en dispositivos médicos, en el sector aeroespacial, en programas de traducción automática de lenguaje natural, etc. En todo caso, la complejidad de las invenciones y el hecho de que tomen como presupuesto programas y aplicaciones informáticas plantea la necesidad de contemplar de forma particularizada, desde un punto de vista jurídico, este tipo de invenciones.

Por otra parte, los programas de ordenador se han protegido tradicionalmente a través del derecho de autor, sobre la base de que el *software* es una mera creación intelectual, no del tipo de las invenciones técnicas, que, en la medida en que está escrito en un código es similar a una obra literaria. Así, se manifiesta expresamente el artículo 1 de la Directiva 24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador cuando declara que *«…los Estados miembros protegerán mediante derechos de autor los programas de ordenador como obras literarias tal y como se definen en el Convenio de Berna para la protección de las obras literarias y artísticas»*. Se trata de un método de protección que resulta sencillo, por cuanto no es preciso el registro ni tampoco por tanto la renovación, requiriéndose únicamente que la obra sea original. Y anudado a lo anterior, de bajo coste. No obstante lo anterior, se trata de una protección que se ha calificado como imperfecta, incompleta y obsoleta. La cuestión, con todo, como con acierto se ha señalado, es que no se trata de un

debate jurídico, sino de carácter económico. No se aprecia ningún obstáculo de carácter jurídico en la legislación sobre derechos de autor que impida proteger los programas de ordenador a través de patentes (96) .

Finalmente, es posible recurrir al secreto empresarial, habida cuenta de que las patentes tampoco permiten proteger por completo el sistema, en la medida que no protegen las compilaciones de datos, como los conjuntos de capacitación en IA, la expresión particular del código fuente de un programador u otro tipo de información patentada que puede ser competitivamente ventajosa y constituir un secreto empresarial. Resulta claro que no toda la información secreta en posesión de una persona es protegible dentro de esta categoría. Habría que diferenciar aquella información relativa a los aspectos íntimos y familiares, de aquella otra que se pretende mantener en secreto porque de ella se deriva una ventaja económica o competitiva. Es sobre esta última, sobre la que podría recaer el secreto empresarial, aun cuando algún autor, se ha llegado a mostrar partidario de introducir contratos de confidencialidad muy parecidos a los utilizados en la cesión o licencia de secretos empresariales para proteger los datos de carácter personal (97) .Cabe, no obstante preguntarse si la opción del secreto empresarial para evitar las dificultades de patentar la IA utilizada de forma generalizada puede finalmente suponer un menoscabo a la innovación y al progreso en general, que son los pilares en los que se ha fundamentado tradicionalmente la protección de las invenciones a través de patentes.

Sea de una u otra forma, la existencia de un derecho de propiedad intelectual a favor del creador del sistema, impide que se pueda tener acceso al código fuente.

Por otra parte, del mismo modo que sucede con las invenciones, los diseños industriales pueden ser generados con la asistencia de sistemas de IA; pero también, lo que sucede cada vez con mayor frecuencia, pueden ser generados de forma autónoma mediante tales sistemas. En el primer supuesto, no parece haber mayor problema en la aplicación de la normativa existente. No deja de ser una actualización desde un punto de vista tecnológico del diseño asistido por ordenador que se viene utilizando desde hace tiempo. La problemática se presenta en el segundo supuesto, y plantea los mismos interrogantes que en los supuestos de invenciones generadas directamente por un sistema de IA.

Desde el Parlamento Europeo (98) se enfatiza la importancia de un sistema efectivo que permita el desarrollo de la IA y con ello, el registro de las patentes y los nuevos procesos creativos. Teniendo en cuenta que el desarrollo de la IA y las tecnologías conexas dependen, en buena medida, de contenidos existentes con anterioridad y de grandes volúmenes de datos, se hace preciso diferenciar con claridad el tratamiento de los datos personales, respecto de los datos no personales. Mientras que con estos segundos se incentiva su intercambio como medida de impuso de la innovación; en relación con los datos personales se recalca la necesidad de una gestión específica en términos de transparencia de los datos en todo el ciclo de vida de un sistema basado en IA (99) . Aunque los propios sistemas de IA pueden servir para mejorar el respeto de los derechos de propiedad intelectual dada su potencialidad, se considera esencial, «la verificación revisión por seres humanos», especialmente si se derivan consecuencias jurídicas (100) .

No parece, en este contexto, que el derecho de protección de datos, ni tampoco el derecho de intimidad, puedan cumplir realmente su función. Cabría pensar en otro derecho, pensado precisamente para este contexto digital, como es el derecho de explicación consagrado en los artículos 13 a15 RGPD. El tema, es como se puede luchar contra la «opacidad» y «discriminación del algoritmo», generado gracias a la IA (en particular, de la *machine learning*) y que se ha nutrido de datos obtenidos de fuentes diversas y tratados oportunamente. La transparencia en forma de «derecho a una explicación» ha surgido como un remedio convincente y atractivo, ya que promete intuitivamente abrir la «caja negra» algorítmica para promover el desafío, la reparación y, con suerte, una mayor responsabilidad (101) .

No obstante, resulta poco probable que el derecho a una explicación en el Reglamento General de Protección de Datos (RGPD) presente un remedio completo a los daños algorítmicos, especialmente en algunas de las principales «historias de guerra algorítmica» que se han vivido en los últimos años (102) . En primer lugar, la ley es restrictiva, poco clara o incluso paradójica en lo que respecta a cuándo puede activarse cualquier derecho relacionado con la explicación. En segundo lugar, la concepción legal de las explicaciones como «*información significativa sobre la lógica del procesamiento*» puede no ser facilitada precisamente por el tipo de «*explicaciones*» que los informáticos han desarrollado, en parte como respuesta para esquivar las preocupaciones de los desarrolladores sobre la divulgación de la propiedad intelectual o los secretos empresariales (103) .

Podría, sin embargo, analizarse el papel que en este ámbito pueden jugar algunos de los mecanismos introducidos por el RGPD, como los previstos en el artículo 22 (104) y 15.h RGPD (105) , en particular los requisitos obligatorios de Privacidad por Diseño y las evaluaciones de impacto de la protección de datos (*Data Protection Impact Asessments,* DPIAs (106)). El objetivo debe ser la creación de mejores algoritmos, así como en formas creativas para que los individuos se aseguren de la gobernanza algorítmica, por ejemplo, mediante la certificación del rendimiento, o de los profesionales que construyen o utilizan algoritmos. Partir de la noción de crear mejores sistemas, con menos opacidad, pistas de auditoría más claras, diseñadores bien formados y holísticos, y la aportación de los públicos interesados parece al final más eficaz que perseguir contra viento y marea una versión «significativa» del interior de una caja negra (107) .

Algunas de estas líneas maestras son las que aparecen recogidas en el proyectado Reglamento Europeo sobre IA titulado provisionalmente Reglamento sobre un enfoque europeo para la IA (*Regulation on a european approach for artificial intelligence*) sobre inteligencia artificial, al que se aludirá con mayor detenimiento en el último apartado de este trabajo.

2. Los robots y la titularidad de derechos de propiedad intelectual

Como se ha señalado, la robótica es una de las categorías de la IA más avanzadas (108) . Su potencialidad es muy amplia en cuanto a las funciones y ámbitos en los que puede actuar. En torno a la misma, se suscitan tanto cuestiones de orden ético como jurídico, relacionadas con los derechos de propiedad intelectual, así como con la privacidad de las personas.

En el informe con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas de 10 de octubre de 2020 (109) se propone una inteligencia artificial «antropocéntrica «, esto es, que los sistemas deben garantizar en todo momento una supervisión humana integral, y «antropogénica», que implica que las tecnologías deben poder permitir en cualquier momento restablecer el control humano, incluso mediante la desactivación de esas tecnologías.

La segunda cuestión, es si ese robot, puede ser considerado inventor y su creación, patentable. Se trata de una cuestión que ya se ha planteado; bien es cierto que por una serie de expertos en IA y patentes para ver cuál podría ser la respuesta de las diferentes oficinas de propiedad intelectual. En concreto se presentaron ante la EPO las solicitudes de patente EP 18 275 163 y EP 18 275 174 figurando el robot DABUS (Artificial Inventor Project) como inventor. La EPO, tomando como base el artículo 81 y la regla 19(1) del Convenio de Patente Europea rechazó las solicitudes. De acuerdo con esta última «*La designación del inventor deberá efectuarse en la solicitud de concesión de patente europea. Sin embargo, si el solicitante no fuese el inventor o el único inventor, la mención deberá realizarse en un documento presentado por separado, en el que constarán el apellido, el nombre y la dirección completa del inventor (…)*». La EPO considera, y de este modo no entra en el fondo del asunto-

que cuando se alude al nombre y apellidos se alude a tributos que no pueden cumplirse con un requisito formal de ponerle un nombre al robot en cuestión, sino que tal requisito forma parte de su personalidad y es el que lo capacita para ejercer sus derechos; entre esos derechos, el ser designado como inventor. El Parlamento, en su resolución de 20 de octubre de 2020, en materia de responsabilidad civil (110) se pronuncia de forma clara al respecto, señalando que «*no es necesario atribuir personalidad jurídica a los sistemas de IA*».

Cabría preguntarse igualmente si las creaciones generadas únicamente por sistemas basados en IA podrían ser protegidas como derechos de autor (111) . Existen ya casos de la denominada IA fuerte, que puede crear de forma autónoma, tanto en el entorno científico, como en el literario y artístico, y en todas las ramas. Ante el avance vertiginoso de estos sistemas, se hace especialmente urgente determinar si esas creaciones que no tienen su origen en el intelecto humano, son protegibles, y quien debe ser considerado el titular de esa creación. Es evidente, como ya se ha señalado, que resulta muy importante para el avance del sector contar con seguridad jurídica y con mecanismos que protejan la creación. Pero también entran en juego, aspectos de carácter ético, así como los relativos a la protección de los derechos fundamentales.

En la Directiva 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE, no se aprovechó la oportunidad para delimitar qué debe entenderse por autor en un contexto digital. Por su parte, en el Texto Refundido de la Ley de Propiedad Intelectual se parte de la consideración del autor como la «*persona natural que crea alguna obra literaria, artística o científica*» (art. 5), si bien se admite en casos concretos la posibilidad de que se beneficien ciertas personas jurídicas de la protección otorgada al autor (art. 10) (editoras, productoras, entre las que no se encuentran las generadas por un sistema de inteligencia artificial. Por su parte, el art. 97.2 en relación con los programas de ordenador establece que puedan ser considerados obra colectiva a tenor del art. 8, tendrán la consideración de autor, salvo pacto en contrario, «*la persona natural o jurídica que la edite y divulgue bajo su nombre*».

Por tanto, se considera autor de una obra protegida por derechos de autor una persona natural, salvo la mención anteriormente referida a las personas jurídicas, lo que sucede en términos similares en otros países como Francia y Alemania, e incluso en Estados Unidos. La doctrina ha defendido esta posición sin fisuras. No obstante, comienzan a barajarse desde la doctrina diferentes construcciones dirigidas a encontrar una solución legal en este ámbito (112) . Las más controvertidas tienden a considerar que debería conferirse la condición de autor de la obra al robot que la crea, partiendo de la consideración de que pudiera ostentar una suerte de personalidad jurídica. Frente a estas, se encuentran los que opinan que no es posible proteger este tipo de creaciones a través de los derechos de propiedad intelectual. Y finalmente, en un camino intermedio, que, en mi opinión, merece ser explotado, se platean diferentes opciones: por un lado, considerar que sería preciso crear un estatuto jurídico propio para las creaciones de IA, distinto al del derecho de autor, en el que no se haría una referencia a obras, sino a «resultados», respecto de los cuales se podría otorgar facultades de explotación económica (113) . Se trata de una opción atractiva, frente a la que se ha objetado, no obstante, que privaría de incluir esas creaciones dentro del marco de los derechos de autor, lo cual tiene ventajas, como es la posibilidad de aplicar una serie de principios comunes, entre los que cabe aludir a la necesidad de lograr un equilibrio entre los intereses del titular y el interés general de acceso a los mismos. También se ha apuntado a la posibilidad de optar por crear un derecho *sui generis* parecido al que se otorga a los fabricantes de bases de datos, o a los editores de obras no protegidas por derechos de autor (114) .

Y existe una cuestión adicional, que únicamente se deja apuntada, tiene que ver con los derechos de autor de aquellas obras «utilizadas» por los sistemas de IA para entrenar o alimentar a los algoritmos que, como hemos visto, son la base sobre la que se asienta la IA. Se trata de un tema fundamental, en el que desde la Unión Europea comienzan a darse tímidos pasos. En particular, en la Directiva 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital ya se alude a que «*en los ámbitos de la investigación, la innovación, la educación y la conservación del patrimonio cultural, las tecnologías digitales permiten nuevos tipos de usos que no se encuentran claramente enmarcados por las normas vigentes de la Unión sobre excepciones y limitaciones. Y además, el carácter optativo de las excepciones y limitaciones establecidas en las Directivas 96/9/CE, 2001/29/CE, y 2009/24/CE podría en esos ámbitos afectar negativamente al funcionamiento del mercado interior, especialmente en el caso de los usos transfronterizos, que ocupan un lugar cada vez más importante en el entorno digital*» (Considerando 5º). Así, se define la minería de textos y datos, como «*toda técnica analítica automatizada destinada a analizar textos y datos en formato digital a fin de generar información que incluye, sin carácter exhaustivo, pautas, tendencias o correlaciones*» (art. 2.2).

Y se establecen en los artículos 3 y 4 de la Directiva medidas para adaptar las excepciones y limitaciones al entorno digital y transfronterizo, si bien todavía con unos fines muy limitado. En la Resolución del Parlamento de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial, Una de las cuestiones a resolver, es a quién pertenece la propiedad intelectual de una creación artística que se ha desarrollado íntegramente con IA, mediante robots o agentes artificiales. En este caso, la opción es evitar la posibilidad de que se puedan acoger a la protección mediante derechos de autor, dado que el principio de originalidad sobre el que se asienta esta protección está anudado a la persona física, y el del a creación intelectual implica la personalidad del autor.

IV. Claves en la regulación de la IA como motor de progreso: una IA fiable y centrada en el ser humano

Tal y como hemos tenido ocasión de señalar, los sistemas de IA, y su protección jurídica a través de derechos de propiedad intelectual pueden en ocasiones suponer una colisión con ese derecho a la privacidad en la era digital, y que supone una conjunción de los derechos de protección de datos y de la intimidad personal y familiar; y, con carácter general, como se recoge en la generalidad de los pronunciamientos de la Unión Europea en este ámbito, a pesar de sus innumerables ventajas pueden conllevar un menoscabo de las libertades y derechos fundamentales. Esto debe conciliarse con el hecho de que desde la propia Unión Europea, como se recoge en la Estrategia Europea de Datos, se incentive el intercambio de datos como mecanismo necesario para el desarrollo tecnológico, y por tanto, económico y social. El desarrollo de la IA también depende de una estrategia de datos eficaz. Para evitar los posibles errores y sesgos de la IA una de las formas más eficientes es garantizar, hasta donde sea legalmente posible, que se puede disponer del mayor volumen posible de datos para el entrenamiento y aprendizaje automático de los sistemas. De datos no personales; pero también, según los casos y atendiendo a fines de interés general, también personales.

Por esta razón, si la premisa es que la IA es necesaria para el progreso, y que para que esta se desarrolle resulta precisa su protección, la necesidad de una regulación que permita compatibilizar ambos aspectos se muestra cada vez más imperiosa.

Conseguir ese equilibrio es uno de los objetivos inspiradores del proyectado Reglamento Europeo sobre IA titulado provisionalmente Reglamento sobre un enfoque europeo para la IA (*Regulation on a european approach for artificial intelligence*) (115) . El Reglamento se considera el instrumento óptimo para lograr un mínimo uniforme de regulación necesario para evitar la fragmentación existente, teniendo en cuenta que la misma supone un importante hándicap para el desarrollo de la innovación basada en IA. Se trata de alcanzar uno de los objetivos previstos en el *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza*, que es, que la IA sea fiable. Por ellos se tienen especialmente presentes las *Directrices para una IA fiable elaboradas por el grupo de expertos de alto nivel sobre la IA* (116) , en las que

se da cuenta de los siete requisitos que resultan esenciales para generar una IA fiable (117) .

La propuesta de Reglamento se basa en los valores y derechos fundamentales de la Unión Europa y tiene como objetivo lograr la confianza de los ciudadanos en el uso de soluciones basadas en IA, además de que dotar de un marco de seguridad jurídica a las empresas para que desarrollen este tipo de soluciones. No en vano, desde el propio Consejo de la Unión Europea en sus Conclusiones «La carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital (118) » instaban a establecer un marco jurídico específico para la IA que permita garantizar el respeto de los derechos fundamentales consagrados en la Carta de Derechos Fundamentales.

Se trata de un Reglamento de mínimos, opción que debe ser saludada, puesto que debe evitarse introducir excesivos obstáculos que pudieran resultar desproporcionados para las empresas y por tanto, llegar a impedir el desarrollo de los sistemas basados en IA. La propia Exposición de Motivos alude a que su objetivo es introducir un enfoque proporcionado, a la par que flexible y que resulte coherente con la Carta de Derechos Fundamentales de la Unión Europea y el Derecho derivado de la Unión en materia de protección de datos.

El Reglamento, que tiene vocación de permanencia, opta por una definición muy amplia de IA, acorde con la rapidez en la evolución de estos sistemas. Y establece una clasificación en las prácticas de IA, basado en un enfoque basado en los riesgos que determina la existencia de un mayor control y supervisión o incluso su prohibición. Así se diferencian las actividades prohibidas, las de alto riesgo, las de riesgo medio/bajo y el resto de sistemas teniendo en cuenta los riesgos que generan y que pueden resultan inaceptables, altos o mínimos por ser contrarios a los valores de la Unión Europea.

Los sistemas de IA prohibidos son aquellos que implican un riesgo inaceptable para la seguridad, la vida y los derechos fundamentales. Entre ellos se recogen diferentes sistemas, como los que tienen un gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que sean capaces de aprovechar las vulnerabilidades de grupos vulnerables concretos, o los que impliquen la identificación biométrica o la videovigilancia masiva en directo por autoridades en espacios públicos, salvo autorización (119) . Los sistemas de riesgo medio/bajo no suponen un riesgo importante para los derechos y libertades. Entre ellos se encontrarían tecnologías como asistentes virtuales que resultan de menor satisfacción. Estos sistemas y el resto que no entran en ninguna de las categorías no tienen obligaciones específicas, y quedarían sujetos a la voluntariedad en la adhesión a códigos de conducta.

De especial interés resulta la regulación de los sistemas de IA que acarrean un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas. Conviene señalar que la clasificación de un sistema de IA como de alto riesgo no depende únicamente de la función que lleve a cabo, sino también de la finalidad específica y de las modalidades para las que se use dicho sistema. En consonancia con un enfoque basado en los riesgos, su admisibilidad está condicionada al cumplimiento de una serie de requisitos obligatorios, estando sujetos a una evaluación de la conformidad *ex ante*, que varía dependiendo del tipo de sistema de IA que se utilice: las que sirven para la identificación biométrica y para el funcionamiento de infraestructuras críticas requieren una verificación previa por un experto independiente; por el contrario, las que se usan con carácter «predictivo» que son las más extendidas, como es el caso de las utilizadas para contratación de trabajadores o su promoción dentro de la empresa, la concesión —o denegación— de créditos, la concesión de prestaciones sociales o las creadas para ser usadas por el poder judicial. Respecto a estas no se exige verificación de terceros sino un control por parte de fabricantes y proveedores, en lo que podría equipararse, salvada la distancia, a una suerte de declaración responsable.

En cuanto a los requisitos, señala la propuesta de Reglamento que deben estar basadas en datos «*que deben ser pertinentes, representativos, que carezcan de errores y completos*» (artículo 10). Es preciso documentar y archivar los datos generados en la creación y utilización de la aplicación (artículo 11). Los sistemas deben estar diseñados de modo que puedan registrar de forma automática eventos (*archivos de registro*) mientras estén funcionando (art. 12). De este modo, garantizarán un nivel de trazabilidad del funcionamiento del sistema de IA durante todo su ciclo de vida. Esto significa que debe disponerse de información sobre el modo en que el sistema se ha desarrollado y su funcionamiento en todo su ciclo. Y para ello es necesario disponer información que quede registrada sobre las características y capacidades y limitaciones del sistema; algoritmos, datos, procesos de entrenamiento, prueba y validación y sobre el sistema de gestión de riesgos.

Asimismo, el sistema debe contar con un grado de transparencia *suficiente* (artículo 13) (120) . En este sentido, en la medida de lo posible —puesto que ya se ha indicado que en muchas ocasiones no lo es— debe aportarse la explicabilidad del proceso de toma de decisiones algorítmico, adaptada a las personas afectadas. Debe proseguirse la investigación en curso para desarrollar mecanismos de explicabilidad. Además, deben estar disponibles las explicaciones sobre el grado en que un sistema de IA influye y configura el proceso organizativo de toma de decisiones, las opciones de diseño del sistema, así como la justificación de su despliegue (garantizando, por tanto, no solo la transparencia de los datos y del sistema, sino también la transparencia del modelo de negocio). Se trata en definitiva de que no haya discriminación ni sesgos contrarios a la equidad (121) .

Esa transparencia *suficiente* se concreta también en que debe resultar compatible con el *cumplimiento de las obligaciones legales del usuario y del proveedor*. Este aspecto, sin duda, es uno de los más complicados a la hora de buscar el equilibrio pretendido por el legislador. Se le pide, por un lado, al proveedor que señale cómo funciona la aplicación, así como los presupuestos de partida o una descripción de los datos que se hayan utilizado para su creación, pero no se le exige transparencia total sobre el *software* utilizado. Entre esas obligaciones, por tanto, también debería incluirse la de respetar los secretos empresariales utilizados en la aplicación de IA. Se señala en este sentido en la Exposición de Motivos que las obligaciones que exigen una transparencia mayor tampoco «afectan de manera desproporcionada» al derecho a la protección de la propiedad intelectual dado que solo se van a aplicar a los requisitos de información mínima necesaria para permitir a las personas que ejerzan su derecho a una compensación efectiva. En todo caso, la transparencia debe conciliarse con la privacidad y la protección datos (122) .

Además, debe quedar siempre sometida a la vigilancia humana (123) (artículo 14). Esto supone que el sistema debe contemplar limitaciones operativas que él mismo no podría desactivar, quedando esta posibilidad reservada únicamente al operador humano y a las personas físicas a las que se haya encomendado la vigilancia del sistema. Esto exige dotar a estos sistemas de una «herramienta de interfaz humano-máquina adecuada». Las medidas para que pueda llevarse a cabo deberán estar definidas, y cuando sea técnicamente posible integradas en el sistema-antes de su introducción en el mercado o puesta en servicio; en todo caso, deberán ser adecuadas para que las lleve a cabo el usuario, si no es posible su integración. Esta vigilancia debe conducir a la posibilidad de rendir cuentas, uno de los aspectos considerados esenciales para que la IA resulte fiable y que viene recogida en las Directrices elaboradas por el grupo de expertos a que hicimos referencia con anterioridad. Se trata de instaurar mecanismos que garantices la rendición de cuentas de los sistemas de IA y de sus resultados, tanto antes como después de su implementación (124) . Para esta categoría de aplicaciones de alto riesgo, el Reglamento establece que son los propios proveedores (arts. 16 a 23) y los fabricantes (art. 24) —no un tercero— los que deben controlar el cumplimiento de estos requisitos.

Por tanto, desde el Reglamento se apuesta por una «innovación responsable» cuando nos encontremos con fines de interés general, entre los que se encuentran lógicamente la protección de los derechos fundamentales. La obligación de realizar pruebas *ex ante*, la gestión de los riesgos y la

vigilancia humana son claves para reducir los riesgos de menoscabo de los derechos fundamentales, y entre ellos los de intimidad y protección de datos, en definitiva la privacidad de las personas. Y ello, porque permiten reducir en gran medida el riesgo de que se tomen decisiones basadas en sistemas de IA que introduzcan sesgos o errores en materias muy importantes, como el empleo, la educación, o en su utilización por los gobiernos o por el poder judicial. Son obligaciones que marcan máximos, aun cuando el Reglamento como ya se ha indicado, es de mínimos. La cuestión es que no parece que resulte nada sencillo concretar en la práctica esas obligaciones. Tampoco su ejecución, dada la opacidad de los algoritmos y su capacidad según los tipos para un comportamiento autónomo de los algoritmos. Habrá que determinarse en cada supuesto cómo se pueden cumplir los objetivos señalados en el Reglamento.

En todo caso, y esto es una cuestión que también contempla la propuesta de Reglamento, las medidas deberán ser acordes con el tipo de organización o de empresa. La opacidad de los algoritmos de la que ya se ha hablado, y la autonomía de los sistemas de IA podrían dificultar, hasta el punto incluso de impedir en la práctica la trazabilidad de las acciones de los sistemas de IA, especialmente en los sistemas basados en redes neurorales y *machine learning*. De ahí la importancia igualmente de la rendición de cuentas y de definir la responsabilidad de las distintas personas que dentro de la cadena, crean, mantienen o controlan el riesgo que se deriva del sistema de IA. Esto lleva a plantear la necesaria revisión de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, donde deben ser redefinidos los principales conceptos: tanto el daño, como el de defecto, como el de productor. Aspecto clave igualmente es el relativo a la responsabilidad civil del operador. Para ello un aspecto que se demuestra central es determinar cómo se puede acceder a los datos que los sistemas recogen o almacenan, y como se pueden auditar sin que ello suponga un menoscabo del derecho a la intimidad.

Por otro lado, debe tenerse claro que el cumplimiento de los requisitos establecidos en el Reglamento no significa que las aplicaciones de IA se puedan utilizar para cualquier cometido y sin mayor control. Es preciso que se concilie con la normativa existente, especialmente la normativa sobre protección de datos, así como en su caso, la que resulte aplicable al sector concreto en el que se vaya a implementar el sistema de IA. Y como se ha indicado, aquí es donde pueden verse contradicciones y aspectos que harán necesario conciliar los diferentes intereses en juego.

En este sentido, debe tenerse en cuenta que el Parlamento aprobó su propuesta sobre legislación de datos el 25 de marzo de 2021. Y también se encuentra en fase de revisión la Convención 108, y en particular, su artículo octavo relativo a la protección de datos. La idea (125) es establecer el derecho explícito de toda persona a no ser sometida a una decisión que le afecte significativamente y que esté únicamente basada en un sistema automatizado de procesamiento de datos sin que se tengan en cuenta sus opiniones; el derecho a obtener conocimiento del razonamiento subyacente al procesamiento de datos cuando se le apliquen los resultados de tal procesamiento; y poden oponerse, en cualquier momento, por motivos relacionados con su situación, al tratamiento de los datos personales que le conciernen, salvo que el responsable del tratamiento tenga motivos legítimos para el tratamiento que anulan su o sus intereses o derechos y libertades fundamentales. Esta propuesta de modernización en realidad está dirigida a crear salvaguardias complementarias en materia de transparencia (artículo 7bis), así como en la necesidad de un examen del impacto probable del procesamiento de datos en los derechos y libertades fundamentales de la persona antes de comenzar dicho tratamiento (artículo 8bis).

Finalmente, una de las medidas para fomentar la innovación basada en IA son la creación de espacios controlados de pruebas (art. 53 Propuesta Reglamento). Ello permitirá tratar datos personales legalmente recopilados con otros fines con la finalidad de desarrollar y probar sistemas innovadores de IA y que estén dirigidos a proteger un interés público esencial en concretos ámbitos, siempre que se cumplan una serie de condiciones. Entre ellas que no se pueda conseguir esos resultados con datos anonimizados, que existan mecanismos para detectar si pueden producirse riesgos elevados para los derechos fundamentales, que el tratamiento de los datos no determine decisiones que afecten a los interesados, que haya una estructura sólida de seguridad de los datos y de documentación de los procesos.

V. Bibliografía

«Algorithms and human rigts». Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Committee of experts on Internet Intermdiaries (MSI_NET). Council of Europe Study DGY (2017) (12). Disponible en : https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

Anexo a la Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones —Plan coordinado sobre la inteligencia artificial 7.12.2018, www.ipex.eu/IPEXL-WEB/dossier/files/./082dbcc5679fb7b40167a1b3f76300c1.do).

ARRABAL PLATERO, P.: *La prueba tecnológica: aportación, práctica y valoración*, Valencia 2020, págs. 168-172.

BARRIO ANDRÉS, A: *Manual de Derecho Digital*, Valencia 2020.

BARRIO ANDRÉS, M., «Del derecho de internet al derecho de los robots» en AAVV (Dir. BARRIO ANDRÉS, M.): *Derecho de los robots*, Madrid 2018, págs. 61-86, págs. 56-58.

BASDEVANT, A.: La discrimination algorithmique en AA.. (DIR. G´sell): *Le big data et le droit*, Paris, 2020, págs. 239-248.

BYGRAVE, LEE. «Article 22. Automated individual decisión-making,including profiling» en AAVV (Dir. KUNER, BYGRAVE, DOCSEY), Oxford, 2020,págs. 522-542.

BYGRAVE, LEE./TOSONI, L, «Article 4(2). Personal data» en AAVV (Dir. KUNER, BYGRAVE, DOCSEY), Oxford, 2020, págs.103-115.

CASTILLO PARRILLA, J.A. «Los datos personales como contraprestación en la reforma del TRLGDCU y las tensiones normativas entre la economía de los datos y la interpretación garantista del RGPD», La Ley Mercantil 82(2021), Págs. 1-23. Consultado en Smarteca.

CLIFFORD, R.D. «Intellectual Property in the era of creative computer program: Will the true creator please stand up? », Tulane Law Review, 71 6(1991), p Disponible en: https://scholarship.law.umassd.edu/cgi/viewcontent.cgi?article=1077&context=fac_pubs ás. págs.1675-1703

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones. Una estrategia Europea de Datos, 19.2.2020. Com (2020) 66 final.

Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones- IA para Europa de 25 de abril de 2018.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y social europeo y al Comité de las regiones. Una estrategia para el Mercado Único Digital de Europa. COM(2015) 192 Final.

Council of Europe, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 17 January 2017, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f06d0 (last visited

on 25 September 2017).

DE LA QUADRA SALCEDO, T.: «Retos, riesgos y oportunidades de la sociedad digital», AAVV (Dir. DE LA QUADRA-SALCEDO,T./PIÑAR MAÑAS, J.L). *Sociedad Digital y Derecho,* Madrid, 2018, págs. 21-86.

DELMAS-LINEL, B./DUMAS G.,» L´impact du RGPD sur les innovations en matière d´IA» *en* AAVV *(dir. G,SELL): Le big data et le droit,,* París, 2020, págs.207-217.

DÍAZ REVORÍO, J. Los Derechos Humanos ante los nuevos avances Científicos y Tecnológicos. Genética e Internet ante la Constitución, Derecho y tic´s. Valencia, 2009.

Digital Globalitation. The new era of global flows. March 2016. McKinsey Global Institute. Disponible en : https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#

Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Explanatory Report1.

DUHIGG,C. : «*Which means that the key is to reach them earlier, before any other retailers know a baby is on the way*»..C. During. «How companies Learn Your Secrets», New York Times, 16 feb. 2012. Disponible en https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

E N N E S Z E/ YU-HSI N C H E N/ TIEN-JU YANG/ JOEL S. EMER:» Efficient Processing of)Deep Neural Networks: A Tutorial and Survey», Proceedings of the IEEE, 105 (2017), Disponible en https://ieeexplore.ieee.org/document/8114708, pág. 2296).

EDWARDS, LILIAN/ VEALE, MI.:, «Slave to the Algorithm? Why a «Right to an Explanation» Is Probably Not the Remedy You Are Looking For (May 23, 2017). 16 *Duke Law & Technology Review 18 (2017),* págs.18-84. Disponible en https://ssrn.com/abstract=2972855 o r http://dx.doi.org/10.2139/ssrn.2972855

EPO-Guidelines2018- GII. 3.6, disponible en https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_6.htm).

European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI).

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL).

European Patent Office, Patents and the Fourth Industrial Revolution. The inventions behind digital transformation | December 2017, pág. 14.). Disponible en: http://documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/$File/fourth_industrial_revolution_2017__en.pdf

FERNÁNDEZ —SAMANIEGO, J./ PIÑAR GUZMAN, B. «Drones y privacidad» en AAVV (Dir. DE LA QUADRA-SALCEDO,T./PIÑAR MAÑAS, J.L). *Sociedad Digital y Derecho*, Madrid, 2018, págs. *359-374.*

FLORES LÓPEZ,L./FERNÁNDEZ PERNÁNDEZ, H.M: *Las redes neuronales artificiales. Fundamentos teóricos y aplicaciones prácticas,* Madrid, 2008.

G´SELL F. «Les décisions algorithmiques», en AAVV. (dir. G´SELL F*): Le big data et le Droit*,,Paris 2020, págs..87-109, pág. 89.

GALLEGO SÁNCHEZ, E., «La patentabilidad de la inteligencia artificial. Otros sistemas de protección». En AAVV. (Dir. MUÑOZ PEREZ, A.F.), *Revolución digital, derecho mercantil y Token economía*. pp. 239 – 270, Madrid,2019.

GALLEGO SÁNCHEZ, E./FERNÁNDEZ PÉREZ, N., *Derecho Mercantil. Parte Primera*, Valencia, 2019.

GARCÍA MEXÍA, P.K., *Derechos y libertades, internet y tics*, Valencia.

GARCÍA-PRIETO CUESTA, J., «¿Qué es un robot?» en AA.VV. (Dir. BARRIO ANDRÉS, M..), *Derecho de los robots*, Madrid 2018, págs..25-59, pág.30.

GÓMEZ SÁNCHEZ, Y.: *Derecho constitucional europeo: derechos y libertades*, Madrid, 2005, pag. 499.

GUICHOT E.. «El Derecho público de la crisis económica : transparencia y sector público» en AAVV (BLASCO ESTEVE, A.): *Hacia un nuevo derecho administrativo : actas del VI Congreso de la Asociación Española de Profesores de Derecho Administrativo,* Palma de Mallorca, 11 y 12 de febrero de 2011, Madrid, 2012, págs. 283-387.

HOFFMAN-RIEM, W: *Big Data. Desafíos también para el Derecho,* Cizur Menor, 2018, págs. 59 y ss.

KOKOTT,J. /SOBOTTA, C.: The distinction between privacy and data protection inte jurisprudence of the CJEU and the EcTHR, *International Data Privacy Law*, 4(2013), págs.222-228. Disponible en: https://watermark.silverchair.com/

LATONERO M.: *Governing Artificial Ingelligence. Upaholding Human Rights &Dignity*. https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza.,. Bruselas 19.02.2020, COM (2020) 65 FINAL, Disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf,

LIEVENS, K: «Patenting Artificial Intelligence»*, Patenting AI EPO Munich 30 May, 2018*, disponible en https://e-courses.epo.org/course/view.php?id=151&lang=en).

LOBATO, M. «Los efectos de la patente y de la solicitud de la patente» en AAVV (Dir.BERCOVITZ,A.): *La nueva Ley de Patentes,* Cizur Menor, 2015, págs..277-300, pág. 279.

METCALF, J. «"The Study Has Been Approved by the IRB": Gayface AI, Research Hype and the Pervasive Data Ethics Gap» Pervade Team, November 30, 2017, https://medium.com/pervade-team/the-study-has-been-approved-by-the-irb-gayface-ai-

MYLLY, T., The constitutionalizacion of the European legal order: Impact of human rights on intelectual property en the EU en AAVV. *Research handbook on human rights and intelectual property*, 2016, págs. 103-131.

NAVAS NAVARRO, S. «Derecho e inteligencia artificial desde el diseño. Aproximaciones», en AA. VV. (coor. NAVAS NAVARRO, S.): *Inteligencia*

artificial, Valencia, Tirant lo Blanch, 2017, págs. 23-72, págs.24 y 25).

NAVAS NAVARRO, S., «Obras generadas por algoritmos. En torno a su posible protección jurídica», *RDC* 2(2018), págs. 273-291.

Opportunities on Artificial Intelligence. Study requested by the ITRE commitee. junio 2020. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf

PÉREZ LUÑO, A., *Derechos humanos, Estado de Derecho y Constitución*, Madrid, 11ª ed. 2017, págs. 84 y ss.

PÉREZ LUÑO, A., Las generaciones de derechos humanos ante el desafío posthumanista», en AA.VV. (Dir. DE LA QUADRA-SALCEDO, T./PIÑAR MAÑAS, J.L): Sociedad Digital y Derecho, Madrid, 2018.

PUYOL MONTERO, J: «Big Data», en AA.VV. (coor. PÉREZ BES): *El Derecho de Internet*, Barcelona 2016, págs. 6-86.

RAMALHO, A., «Ex Machine, Ex Auctore? Machines that créate and how Eu copryright law views them, disponible en Http://copyrghtblog.kluweiplaw.com/2018/11/12ex-machines´that´createánd´howéu´copyrighte-law´views-them/;

SAN JUAN RODRÍGUEZ, N., «La inteligencia artificial y la creación intelectual: ¿está la propiedad intelectual preparada para este nuevo reto?» opc.it, pág. 23

Recommendation CM/Rec (2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/7, 23 Mar. 2017

SAMUELSON, P.: «Privacy as intellectual property?», en *Standford Law review,* vol.52 (2000), págs. 1125-1173.

SAN JUAN RODRÍGUEZ, N.: «La inteligencia artificial y la creación intelectual: ¿está la propiedad intelectual preparada para este nuevo reto?» (1), *La Ley Mercantil,* 72(2020), págs. 1-28.

SÁNCHEZ GARCÍA, L., *El inventor artificial. Un reto para el derecho de patentes*, Cizur menor, 2020.

SHEMTOV, N. «When Innovation Innovates: Assessing Inventive Step in Autonomous Inventive Processes», Patenting AI EPO Munich 30 May, 2018, disponible en https://e-courses.epo.org/course/view.php?id=151&lang=en. Sería el caso del Deep Blue de IBM, que solo juega al ajedrez

SNOW, J.,«Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots,» *ACLU,* July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

Study on the human rights dimensions of automated data processing tecniques (in particular algorithms) and posible regulatory implications.

STROWEL, A. «Big Data and data appropriation in the EU», en AAVV. (ed. APLIN,T.), *Research Handbook on Intellectual Property and Digital Technologies, Chelnenham* UK- Northampton, MA.USA, 2020, págs. 107-135.

TUTT, A: «An FDA for algorithms», Administrative Law Review 83 (2017), págs. 83-123. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994, págs.83-123.

VILLARINO MARZO, J. La privacidad en el entorno del cloud computing. Tesis doctoral. Repositorio Universitat Abat Oliva CEU. 2017.

VILLARINO MARZO, J.: *La privacidad en el entorno del cloud computing*, Madrid 2018

WHITMAN, J.Q. «The Two Westerns Cultures of Privacy: Dignity versus Liverty, *Yale Law Review*, marzo (2004), págs. 1151 a 1221.

World Intellectual Property Organization (WIPO). WIPO Technology Trends 2019: Artificial Intelligence. Geneva: World Intellectual Property Organization., p. 143. [Consultado el 13 de mayo de 2020]. Disponible en https://www.wipo.int/edocs/pubdocs/en/wipo_*pub*_1055.pdf

YILUN WANG/ MICHAL KOSINSKI, «Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images,» *Journal of Personality and Social Psychology* (preprint), https://osf.io/zn79k/.

ZANFIR-FORTUNA, G., Article 15. Right of Access by the data subject» en AAVV (Dir. KUNER,C/BYGRAVE,L/DICKSEY, C.); *The EU General Data Protection REgulation (GDPR). A Commentary,* Oxford 2020, págs. 449-468.

(1) Trabajo realizado en el marco del Convenio UA Diputación para impulsar los procesos de innovación, generación y transferencia de conocimientos y tecnología en el ámbito de la inteligencia digital (2020) (conveniointeligenciadigital) y del Proyecto PID2020-118006RB-I00 del Ministerio de Ciencia e Innovación.

(2) CASTILLO PARRILLA, J.A. «Los datos personales como contraprestación en la reforma del TRLGDCU y las tensiones normativas entre la economía de los datos y la interpretación garantista del RGPD», La Ley Mercantil 82(2021), pág. 2 .Consultado en smarteca.

(3) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones. Una estrategia Europea de Datos, 19.2.2020. Com (2020) 66 final, págs. 1-2.

(4) Hay ámbitos, como el de la producción industrial o el del análisis de radiografías a través de ordenador donde los resultados son particularmente significativos. Vid. Al respecto, HOFFMAN-RIEM, W: *Big Data. Desafíos también para el Derecho,* Cizur Menor, 2018, págs. 59 y ss.

(5) Acerca de su significado e implicaciones, STROWEL, A. «Big Data and data appropriation in the EU», en AAVV. (ed. APLIN,T.), *Research Handbook on Intellectual Property and Digital Technologies, Chelnenham* UK- Northampton, MA.USA, 2020, págs. 107-135.

(6) De ahí, que de forma amplia, pueda considerarse que Big Data engloba «*infraestructuras, tecnologías y servicios que han sido creados para dar solución al procesamiento de enormes conjuntos de datos estructurados, no estructurados, o semi-estructurados (mensajes en redes sociales, señales de móvil, archivos de audio, sensores, imágenes digitales, datos de formularios, emails, datos de encuestas, logs, etc) que pueden provenir de sensores, micrófonos, cámaras, escáneres médicos, imágenes*» tal y como indica PUYOL MONTERO, J: «Big Data», en AA.VV. (coor. PÉREZ BES): *El Derecho de Internet*, Barcelona 2016, págs. 6-86, pág.70.

(7) Si la primera revolución industrial vino marcada por el paso de la producción artesanal al desarrollo de la maquinaria y la fabricación en mayor escala, la segunda, por la utilización de la energía eléctrica y la producción masiva en cadenas de montaje, la tercera, por la automatización de la fabricación y la informatización de las empresas industriales, esta cuarta revolución consiste en la introducción de las tecnologías digitales en la industria. Mientras que las revoluciones industriales anteriores han logrado automatizar el trabajo físico, la 4IR va más allá, puesto que se trata de automatizar grupos enteros de tareas, incluyendo tareas intelectuales realizadas por seres humanos. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y social europeo y al Comité de las regiones. Una estrategia para el Mercado Único Digital de Europa. COM(2015) 192 Final.

Se percibe claramente, la existencia de una transición hacia fábricas y dispositivos «inteligentes» que operan de manera autónoma, como se recoge en el Documento *European Patent Office, Patents and the Fourth Industrial Revolution. The inventions behind digital transformation* | December 2017, pág. 14.). Disponible en : http://documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/$File/fourth_industrial_revolution_2017__en.pdf

(8) Digital Globalitation. The new era of global flows. March 2016. McKinsey Global Institute. Disponible en : https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#

(9) DELMAS-LINEL, B./DUMAS G., «L´impact du RGPD sur les innovations en matière d´IA» *en* AAVV *(dir. G,SELL): Le big data et le droit,* París, 2020, págs..207-217, pág- 207.

(10) Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza.,. Bruselas 19.02.2020, COM (2020) 65 FINAL, Disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf, pág. 1, donde se alude a que entre las ventajas que puede reportar a nuestra vida se encuentra por ejemplo la mejora de la atención sanitaria (mejores diagnósticos y mejor prevención de las enfermedades), aumentando la eficiencia de la agricultura, mejorando la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, y con ello la mitigación del cambio climático, y también mejorará la seguridad.

(11) El origen suele situarse en un curso de verano sobre informática teórica que se celebró en Estados Unidos en 1956 (McCARTHY, J; MINSKY, M.L.; ROCHESTER, N.; SHANNON, C.E.: «A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence», August 31, 1955, https://www.open.edu/openlearn/ocw/pluginfile.php/623615/mod_resource/content/1/m366_1_dartmouth.pdf). Allen Newell y Herbert Simon presentaron en él un programa de ordenador, el Logic Theorist, que emulaba características propias del cerebro humano y que ha sido considerado el primer sistema de inteligencia artificial dado que era capaz de demostrar los teoremas sobre lógica matemática recogidos en los tres volúmenes de los *Principia Mathematica* de Alfred N. Whitehead y Bertrand Russell (1910-1913). Puede encontrarse esta y otra información complementaria en NAVAS NAVARRO, S. «Derecho e inteligencia artificial desde el diseño. Aproximaciones», en AA. VV. (coor. NAVAS NAVARRO, S.): *Inteligencia artificial*, Valencia, Tirant lo Blanch, 2017, págs. 23-72, págs.24 y 25). No obstante esta primera afirmación, se ha señalado que el término se debe a John McCarthy, otro de los participantes, quien definió la IA como «*la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes*», lo que equipararía la IA a una rama de las ciencias computacionales encargada de desarrollar modelos capaces de realizar tareas propias de los seres humanos, simulando razonamientos y conductas.

(12) NAVAS NAVARRO, S. «Derecho e inteligencia artificial desde el diseño», op.cit., pág. 24.

(13) Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES

(14) Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, Bruselas 21. 4.2021, COM (2021) 206 Final.

(15) En la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial (2020/2015(INI)), que sirve de base en la elaboración del Reglamento, se señala en su apartado séptimo que **«**la Unión debe abordar las diferentes dimensiones de la IA por medio de definiciones tecnológicamente neutras y suficientemente flexibles, de modo que puedan incluirse los futuros avances tecnológicos, así como usos ulteriores». En esta línea, el Proyecto de Reglamento, en la Exposición de Motivos (considerando 6) señala que «*resulta necesario definir con claridad la noción de sistema de IA para ofrecer seguridad jurídica, al mismo tiempo que se proporciona la flexibilidad necesaria para adaptarse a los futuros avances tecnológicos. La definición debe basarse en las principales características funcionales del software, y en particular en su capacidad para generar, en relación con un conjunto concreto de objetivos definidos por seres humanos, contenidos, predicciones, recomendaciones, decisiones u otra información de salida que influyan en el entorno con el que interactúa el sistema, ya sea en una dimensión física o digital. Los sistemas de IA pueden diseñarse para operar con distintos niveles de autonomía y utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente de él (integrado) o tiene una funcionalidad en el producto sin formar parte de él (no integrado). La definición de 'sistema de IA' debe complementarse con una lista de las técnicas y estrategias concretas que se usan en su desarrollo. Dicha lista debe estar actualizada atendiendo a los avances tecnológicos y del mercado, para lo cual la Comisión debe adoptar actos delegados que la modifiquen*». En esta línea, en el artículo 3 del Proyecto de Reglamento se define de forma amplia como : «*el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa*».

(16) *Opportunities on Artificial Intelligence. Study requested by the ITRE commitee*. Junio 2020. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf

(17) Libro Blanco sobre Inteligencia Artificial, op.cit., pág. 10.

(18) Cita esta expresión por vez primera, McLAUGHLIN, M., «Computer-Generated Inventions» en *Social Science Research Network Electronic Jounal*, enero 2018, pág. 8, según recoge SÁNCHEZ GARCÍA, L., *El inventor artificial. Un reto para el derecho de patentes*, Cizur menor, 2020, pág. 21.

(19) DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T., «Retos, riesgos y oportunidades de la sociedad digital», AAVV (Dir. DE LA QUADRA-SALCEDO,T./PIÑAR MAÑAS, J.L):. *Sociedad Digital y Derecho*, Madrid, 2018., págs. 21-86.

(20) Baste con recordar la sanción impuesta por la APD a Google por prácticas abusivas con su servicio de comparador al dar preferencia a los productos que ella misma comercializa a través de su servicio google-shop, frente a los de otros competidores. O las multas de 300.000 euros impuestas a Whatsapp y a Facebook por el trasvase y el tratamiento de datos personales de usuarios a partir de la compra de la primera por la segunda, en el 2014. De forma similar ha ocurrido en otros países de nuestro entorno, como Francia o Alemania

(21) LOBATO, M. «Los efectos de la patente y de la solicitud de la patente» en AAVV (Dir.BERCOVITZ,A.): *La nueva Ley de Patentes,* Cizur Menor, 2015, págs.277-300, pág. 279.

(22) La ley de Privacidad del Consumidor (CCPA, por sus siglas en inglés), que prevé que, si una empresa compra o vende datos de al menos 50.000 residentes de este estado en un año, o sus ingresos anuales superan los 25 millones de dólares, o el 50% de sus ingresos provienen de la venta de información personal de sus clientes, tiene que revelar qué categorías de datos está recopilando y qué está haciendo con los datos de sus clientes

(23) Algún autor, a pesar de reconocer la diferente naturaleza jurídica de los datos personales y los secretos empresariales, se ha mostrado partidario de introducir contratos de confidencialidad análogos a los utilizados en la cesión o licencia de secretos empresariales, para proteger los primeros. En este sentido *Vid.* SAMUELSON, P.: «Privacy as intellectual property?», en *Standford Law review,* vol.52, 2000, pgs. 1125-1173, 1157 y 1158.

(24) DE LA QUADRA SALCEDO, T.: «Retos, riesgos y oportunidades de la sociedad digital», AAVV (Dir. DE LA QUADRA-SALCEDO,T./PIÑAR MAÑAS, J.L.:. Sociedad Digital y Derecho, Madrid, 2018. pág. 45.

(25) El uso de datos de perfiles, incluidos los establecidos en base a los datos recopilados por algoritmos de búsqueda y motores de búsqueda, afecta directamente el derecho de una persona a autodeterminación informativa. El interesado normalmente no conocerá la a elaboración de perfiles a sí misma y la posterior reutilización de datos más allá de su contexto original, facilitando la búsqueda de información al reducir la oscuridad práctica del anonimato datos. Además, los resultados obtenidos mediante algoritmos de búsqueda pueden estar incompletos, inexacto o desactualizado, colocando así a los individuos en una luz distorsionada, que puede ser perjudiciales. Vid. Algorithms and human rigts». Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Committee of experts on Internet Intermdiaries (MSI_NET). Council of Europe Study DGY (2017) (12), págs. 15-16.

(26) Tal y como salió publicado, el periodista Carles Duhigg desveló como la cadena Target, la segunda más importante de venta a distancia de Estados Unidos, tenía una base de datos sobre mujeres embarazadas con la finalidad de detectar, teniendo en cuenta las compras que hacían, las clientas que podían estarlo. Para ello se tenían en cuenta las compras durante veinte semanas de magnesio o zing, , o la compra de jabones sin perfumes, así como otra serie de indicios. Target estimaba todos esos datos y si una clienta de 23 años los compraba en marzo, podía estimar que en un 87% de los casos la mujer daría a luz en agosto. Señala el periodista «*Which means that the key is to reach them earlier, before any other retailers know a baby is on the way*»..C. During. «How companies Learn Your Secrets», New York Times, 16 febrero 2012.

(27) En la Resolución del Parlamento Europeo de 20 de octubre de 2020 relativa a un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (Parliament resolution with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies) 2020/2012(INL), se alude a la necesidad de garantizar la seguridad, la transparencia y la responsabilidad para evitar cualquier forma de sesgo y discriminación, así como el respeto de los derechos fundamentales. De forma rotunda, se asevera en la misma que «*El ciudadano es el centro de la propuesta*».

(28) Estrategia Europea de los Datos, op.cit., pág. 5.

(29) DE LA QUADRA SALCEDO, T.: «Retos, riesgos y oportunidades de la sociedad digital», op.cit., pág.45.

(30) La Comisión Europea emitió un comunicado el 4 de junio de 2021 anunciando una investigación antimonopolio a Facebook para evaluar si la compañía estadounidense violó las normas de competencia de la UE al utilizar datos publicitarios de anunciantes, a fin de competir con ellos en mercados como el de los anuncios clasificados. También analizará si Facebook vincula su servicio de anuncios clasificados en línea «Facebook Marketplace» a su red social, en incumplimiento de las reglas de competencia de la Unión Europea (UE). Se parte de la consideración de que cerca de 3.000 millones de personas utilizan Facebook sobre una base mensual y casi 7 millones de empresas se anuncian en Facebook en total.

(31) Por ejemplo, los investigadores de la Universidad de Stanford entrenaron una red neuronal profunda para «predecir» la orientación sexual de un grupo de personas, sin obtener el consentimiento, utilizando un conjunto de imágenes recopiladas de sitios web de citas en línea. Vid. YILUN WANG/ MICHAL KOSINSKI, «Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images,» *Journal of Personality and Social Psychology* (preprint), https://osf.io/zn79k/.

(32) Un análisis de los peligros y problemas derivados de la «*vigilancia algorítmica*», donde los datos que se recopilan y analizan pueden ser una amenaza para los usuarios porque permiten revelar información personal puede verse en los trabajos de:METCALF, J. «'The Study Has Been Approved by the IRB»:Gayface AI, Research Hype and the Pervasive Data Ethics Gap,» Pervade Team, November 30, 2017,https://medium.com/pervade-team/the-study-has-been-approved-by-the-irb-gayface-ai-esearchhype-and-the-pervasive-data-ethics-ed76171b882c; PENAGOS, M. «AI Systems and Research Revealing Sexual Orientation Case Study,» AI and Human Rights Workshop, Data & SocietyResearch Institute, April 26-27, 2018, disponible en https://datasociety.net/wp-content/uploads/2018/05/AI-Systems-and-Research-Revealing-Sexual-Orientation_Case-Study_Final_CC.pdf.

(33) Un ejemplo es el software de reconocimiento facial impulsado por IA de Amazon. En julio de 2018, los investigadores de la Unión Estadounidense de Libertades Civiles (ACLU) llevó a cabo un experimento que combinaba fotografías de los 535 miembros del Congreso con una base de datos de 25.000 imágenes públicas de personas detenidas. Los investigadores encontraron que el software no solo produjo 28 coincidencias falsas, pero también tuvo prejuicios raciales. Dado que Amazon ha vendido esto software a los departamentos de policía, la ACLU expresó su preocupación por el uso posterior de tratamientos faciales reconocimiento de la vigilancia gubernamental, que es omnipresente, opaca y no regulada. Vid. Al respecto, SNOW, J.,«Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots» *ACLU,* July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

(34) La propiedad intelectual es una locución técnica que incluye la disciplina de las creaciones industriales (patentes, modelos de utilidad y diseños industriales) de los signos distintivos (marcas, nombres comerciales y rótulos de establecimiento), de los signos distintivos de calidad (denominaciones de origen e indicaciones geográficas) y de los derechos de autor, concebidos todos ellos como creaciones del intelecto humano y, por ende, como bienes inmateriales susceptibles de protección por el Derecho. Se trata de una orientación político-jurídica acorde con la preconizada por la OMPI ya en 1967 y posteriormente ratificada por la Declaración de las partes contratantes del GATT de Punta del Este en 1986. También en otros instrumentos legales como la Directiva 2004/48/CE del Parlamento Europeo y del Consejo de 29 de abril de 2004 relativa al respeto de los derechos de propiedad intelectual o en el Reglamento de la Unión Europea 2015/2424 del Parlamento Europeo y del Consejo de 16 de diciembre de 2015. Vid. con mayor detalle las razones que avalan esta posición en GALLEGO SÁNCHEZ, E./FERNÁNDEZ PÉREZ, N., Derecho Mercantil. Parte Primera, Tirant lo Blanch, 2019, págs.209-211.

(35) MYLLY, T., The constitutionalizacion of the European legal order: Impact of human rights on intelectual propery en the EU en AAVV. *Research handbook on human rights and intelectual property*, 2016, págs. 103-131, pág-103.

(36) Una Estrategia Europea de Datos, op.cit.

(37) Study Human rights,pág. 16. Vid. por todos, VILLARINO MARZO, J.: *La privacidad en el entorno del cloud computing*, Madrid 2018. En particular, en las págs.25-63 alude a los desafíos de esta tecnología.

(38) BASDEVANT, A.: La discrimination algorithmique en AA.. (DIR. G´sell): *Le big data et le droit*, Paris, 2020, págs. 239-248, pág. 240, señala que las leyes en materia de protección de datos ofrecen una protección a priori en virtud de la cual se precisa el consentimiento para un tratamiento lícito de los datos – que lleva implícito un uso legítimo para una finalidad determinada, que sean los datos necesarios y pertinentes, etc. Sin embargo, el respeto a la intimidad, constituye una protección a posteriori para reparar las intrusiones por parte de terceros

(39) Véase al respecto la STC 207/1996, de 16 de diciembre de 1996.

(40) WHITMAN, J.Q. «The Two Westerns Cultures of Privacy: Dignity versus Liverty», *Yale Law Review*, marzo (2004), págs. 1151 a 1221.

(41) Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01). El artículo 7º recoge el «Respeto de la vida privada y familiar» señalando que «*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio*».

(42) El primer texto de derecho en reconocer la «privacidad» fue la Declaración Universal de Derechos Humanos (en adelante DUDH), de 10 de diciembre de 1948 (art. 12), que habla de «vida privada». En el sistema europeo específicamente, encontramos la protección del derecho a la intimidad en el Convenio Europeo de Derechos Humanos (en adelante CEDH), de 4 de noviembre de 1950 (art. 8); en la Carta de Derechos Fundamentales de la Unión Europea (en adelante CDFUE), de 12 de diciembre de 2007 (art. 7).

(43) El Tribunal Constitucional en su STC 231/1988, de 2.12.1988 declaró que: *…el derecho a la intimidad personal y familiar reconocidos en el art. 18 CE aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la «dignidad de la persona» que reconoce el art. 10 CE, y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo «(Fundamento Jurídico Tercero).*

(44) STC 231/1988, de 2 de diciembre de 1988 (Fundamento Jurídico Tercero).

(45) STC 207/1996, de 16 de diciembre, F.J. 3º, b) – *«(…) el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 C.E.), implica «la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana»* (SSTC 231/1988, 197/1991, 20/1992, 9/1992, 142/1993, 117/1994 y 143/1994), y referido preferentemente a la esfera, estrictamente personal, de la vida privada o de lo íntimo (SSTC 142/1993 y 143/1994)».

(46) STC 199/2013, de 5 de diciembre de 2013 (Fundamento Jurídico Sexto); STC 127/2003, de 30 de junio de 2003 (Fundamento Jurídico Séptimo) y STC 89/2006, de 27 de marzo de 2006 (Fundamento Jurídico Quinto); STC 119/2001, de 24 de mayo de 2001 (Fundamento Jurídico Sexto) y STC 134/1990, de 19 junio de 1990 (Fundamento Jurídico Cuarto); STC 136/1989, de 19 de julio de 1989 (Fundamento Jurídico Segundo). El TC insiste en su jurisprudencia que el derecho a la intimidad atribuye a su titular «(…) el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida (STC 231/1988, de 2 de diciembre de 1988 (Fundamento Jurídico Tercero); STC 236/2007, de 7 de noviembre de 2007 (Fundamento Jurídico Undécimo) ; 60/2010, de 7 de octubre de 2010 Fundamento Jurídico Octavo) y por ello , «(…) el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión» 8 en la esfera íntima y la prohibición de hacer uso de lo así conocido . (STC 206/2007, de 24 de septiembre de 2007 Fundamento Jurídico Cuarto).

(47) La STC 196/2004, de 15 de noviembre de 2004 (Fundamento Jurídico Noveno) en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, se reconoce no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad.

(48) Y como ha indicado el Tribunal Constitucional ese consentimiento es revocable en cualquier momento1020, decisión que se impone sobre los terceros que hayan accedido a esa información impidiéndoles su uso. Obviamente, el acceso previo no se torna en intromisión ilegítima una vez revocado el consentimiento, pues éste carece de efectos retroactivos. Ahora bien, deja sin efecto cualquier pacto o negocio jurídico relativo a la revelación de aquella información.

(49) STC 196/2004, de 15de noviembre de 2004 (Fundamento Jurídico Segundo), STC 206/2007, de 24 de septiembre de 2007 (Fundamento Jurídico Quinto); y STC 70/2009, de 23 de marzo de 2009 (Fundamento Jurídico Segundo).

(50) STC 292/2000, de 30 de noviembre de 2000 (Fundamento Jurídico Quinto).

(51) En su artículo 8 se establece: «*Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad correspondiente*».

(52) Se alude de forma muy gráfica, a que los avances en la tecnología determinan que desaparezcan las fronteras que tradicionalmente permitían proteger el derecho a la intimidad. Por un lado, el tiempo, puesto que, al transcurrir, se desvanecía el recuerdo de actividades ajenas, impidiendo «la configuración de una historia lineal e ininterrumpida de la persona». Y la distancia, porque impedía conocer hechos de personas en lugares muy distantes. Frente a esta situación, las modernas técnicas de comunicación, ya en ese momento, en el que todavía no se atisbaban herramientas de Big Data y de Inteligencia Artificial como en la actualidad, se decía en la ley, permiten salvar sin dificultades esos límites. Y por ello, se aludía que frente a la utilización mecanizada, ordenada y discriminada de los datos, debería establecerse una frontera para evitar el menoscabo de la intimidad de las personas. una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución. En ese sentido, mientras que la intimidad está protegida en los tres primeros párrafos de la Constitución y por sus normas de desarrollo, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

(53) Vid. Por todos, los comentarios a diferentes sentencias de ambos tribunales en el trabajo de KOKOTT,J. /SOBOTTA, C., The distinction between privacy and data protection inte jurisprudence of the CJEU and the EcTHR, International Data Privacy Law, 4[2013], págs.222-228. Disponible en: https://watermark.silverchair.com/

(54) DÍAZ REVORÍO, J. Los Derechos Humanos ante los nuevos avances Científicos y Tecnológicos. Genética e Internet ante la Constitución, Derecho y Tic´s. Valencia, 2009, pág. 178.

(55) Con carácter previo, en la sentencia TC 254/1993, de 20.07.1993, se recoge por vez primera el derecho de recurrente a ser informado acerca de la existencia, finalidad e identidad del responsable de us daos en la administración del Estado o en los organismos dependientes de la misma.

(56) STC 292/2000, de 30 de noviembre de 2000 (Fundamento Jurídico Séptimo)

(57) STC 39/2016, de 3 de marzo de 2016 (Fundamento Jurídico Tercero) con referencia a la STC 292/2000, de 30 de noviembre 2000 (Fundamento Jurídico Dieciséis) F.J. 16º.

(58) VILLARINO MARZO, J., La privacidad en el entorno del cloud computing, op.cit., pág. 46, señala que la sustantividad de ambos derechos también se contempla por las autoridades públicas, dado que la AEPD indica que «*puede informar sobre el derecho de protección de datos de carácter personal, también llamado de autodeterminación informativa por el Tribunal Constitucional, y no sobre el derecho a la intimidad y a la propia imagen*».

(59) VILLARINO MARZO, J., La privacidad en el entorno del cloud computing, op.cit.,pág. 47.

(60) La STC 173/2011, de 7 de noviembre de 2011 señala que «*si no hay duda de que los datos personales relativos a una persona individualmente considerados... están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc,) —por lo que sus funciones podrían equipararse a los de una agenda electrónica— , no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser*

humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos sobre su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad e su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo queda afectado en tal caso, no solo el derecho al secreto de las comunicaciones del art 18.3 (por cuando es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1. CE) en la medida en que estos correos o mail, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. O ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular, la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información».

(61) LATONERO M.: *Governing Artificial Ingelligence. Upaholding Human Rights &Dignity*. Disponible en : https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

(62) PÉREZ LUÑO, A., Las generaciones de derechos humanos ante el desafío posthumanista», en AA.VV. (Dir. DE LA QUADRA-SALCEDO,T./PIÑAR MAÑAS, J.L):. Sociedad Digital y Derecho, Madrid, 2018, pág. 138.

(63) Una parte importante de la doctrina constitucionalista alude a la existencia de tres categorías de derechos fundamentales PÉREZ LUÑO, A., *Derechos humanos, Estado de Derecho y Constitución*, Madrid, 11 ed. 2017, págs. 84 y ss. 144-148 Se habla así de una primera categoría en la que los derechos humanos son considerados como derechos de defensa *(Abwehrrechte*) de las libertades de la persona. La segunda categoría, corresponde a los derechos económicos, sociales y culturales, que tienen una traducción en derechos de participación (*Teilhaberechte*), respecto a los que ya se precisa una actuación de los poderes públicos dirigida a garantizar su ejercicio, y que se llevan a cabo a través de prestaciones y servicios públicos. La tercera vendría marcada por la revolución tecnológica; ciertos usos o abusos de la tecnología han dado lugar a nuevas amenazas para los derechos, lo que implica la formulación de nuevos derechos o la actualización de los ya existentes. En esta categoría se incluirían los derechos relativos al medio ambiente, la calidad de la vida y la paz; los derechos en el ámbito de las tecnologías de la información y la comunicación (TIC); y los derechos en la esfera de la bioética y de las biotecnologías.

(64) Para otro sector, que cada vez gana más partidarios, las tres primeras generaciones de derechos son producto de la evolución política, mientras de que la cuarta es producto de la evolución científica y técnica. Tal es así, que por una parte de la doctrina se habla de los «Derechos de cuarta generación», entre el que se incluiría el de la protección de datos: derechos nuevos relacionados con la biomedicina y la genética, y con las tecnologías de la información y la comunicación. Algunos autores consideran que estos derechos son las nuevas formas que cobran los derechos existentes en el entorno del ciberespacio. Otros autores, consideran que entre estos derechos de cuarta generación se incluyen tanto los relacionados con la biomedicina y la genética (identidad genética, integridad genética, consentimiento informado en las intervenciones sobre la salud) y los vinculados a las tecnologías de la información y comunicación (el acceso universal a las TIC, el derecho a la protección de datos personales...). Por lo tanto, comprendería derechos nuevos relacionados con las biotecnologías, y también derechos de generaciones anteriores a los que la tecnología ha impactado de tal modo que sus contornos y por tanto su contenido esencial ha variadoO. En este sentido, VILLAMARINO MARZO, J. La privacidad en el entorno del cloud computing. Tesis doctoral. Repositorio Universitat Abat Oliva CEU. 2017; GÓMEZ SÁNCHEZ, Y.: *Derecho constitucional europeo: derechos y libertades*, Madrid, 2005, pág. 499

(65) Documento elaborado por un grupo de expertos nombrados por el Gobierno, que se presentó el 15 de julio de 2021. Con carácter de recomendación, se enmarca en una tendencia cada vez más generalizada y asumida por los operadores del mercado a favor del *soft law*, lo que le dota de un carácter dinámico, muy acorde con un mundo en constante evolución. El objetivo de la Carta de Derechos Digitales no es consagrar nuevos derechos fundamentales distintos a los ya reconocidos. Se trata, como se establece en la Carta, de perfilar aquellos derechos que resultan más relevantes en un entorno digital y delimitar aquellos otros que resultan instrumentales o auxiliares de los primeros.

(66) En primer término, los derechos de libertad, entre los que se recogen el derecho a la identidad en el entorno digital, el derecho a la protección de datos, el derecho al pseudonimato, el derecho de la persona a no ser localizada y perfilada, el derecho a la ciberseguridad y el derecho a la herencia digital. Se trata de derechos en unos casos plenamente reconocidos, como el de la protección de datos, y en otros, como por ejemplo el de la herencia digital, una adaptación de derechos existentes al nuevo escenario digital.

El bloque de derechos de igualdad supone la aplicación al entorno digital del derecho fundamental a la igualdad. Y entre sus manifestaciones, se incluye el derecho de acceso a internet, el derecho a la protección de las personas menores de edad en el entorno digital, el derecho a la accesibilidad universal en el entorno digital y en la exigencia de que se faciliten y fomenten los medios necesarios para evitar la existencia de brechas de acceso al entorno digital.

El tercer bloque viene constituido por los derechos de participación y de conformación del espacio público. Se trata de un conjunto heterogéneo de derechos. Por una parte, se parte de principio de neutralidad al que deben sujetarse los proveedores de servicios de internet y que ya viene consagrado normativamente; y se reafirman los derechos a la libertad de expresión y de información en entornos digitales, el derecho a recibir libremente información veraz. Por otra, se establece como criterio inspirador para la actuación de los poderes públicos, la necesidad de que se proporcione una educación digital. Y, finalmente, se reconocen los derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas.

En cuarto lugar, encontramos los derechos del entorno laboral y empresarial. Entre ellos, el derecho a la desconexión, digital, al descanso y a la conciliación de la vida personal y familiar; o la necesaria protección de los derechos de las personas trabajadores a la intimidad personal y familiar, el honor y la propia imagen, la protección de datos y el secreto de las comunicaciones en el uso de dispositivos digitales para realizar su trabajo. En relación con las empresas, se contemplan dos aspectos: por un lado, los criterios de actuación que deben guiar su actuación en defensa y promoción de una competencia efectiva, evitando posiciones de dominio en el mercado; y, por otra parte, fomentando los espacios de pruebas controladas (*sandbox*) como vía para propiciar el desarrollo empresarial mediante la creación de nuevas empresas de base tecnológica.

El quinto bloque se refiere a los derechos digitales en entornos específicos. En particular, se abordan, atendiendo a las características singulares o de mayor interés público, algunos ámbitos como es el relativo a las condiciones para acceder a datos con fines de archivo en interés público, fines de investigación, estadísticos y de innovación y desarrollo; el derecho a la protección de la salud en el entorno digital, el reconocimiento del derecho a la libertad de creación y de acceso a la cultura en el entorno digital; y los derechos en el empleo de las neurotecnologías. Finalmente, en se alude a los derechos de las personas a que estos derechos tengan la adecuada tutela administrativa y judicial, para lo que el Gobierno deberá adoptar las medidas oportunas.

(67) *La intimidad personal y familiar se puede vulnerar con drones (vid. FERNÁNDEZ -SAMANIEGO, J./ PIÑAR GUZMAN, B».* Drones y privacidad» en AAVV*, Sociedad digital y derecho pág. 359 y ss (pág. 361*

(68) Vid. Un comentario sobre el concepto de «personal data» y una recopilación de casos en el comentario de BYGRAVE, LEE./TOSONI, L, «Article 4(2). Personal data en AAVV (Dir. KUNER, BYGRAVE, DOCSEY), The EU General Data Protection REgulation (GDPR). A Commentary, Oxford, 2020 págs. 103-115.

(69) VILLARINO MARZO, J., La privacidad en el entorno del cloud computing, op.cit pág. 134

(70) GUICHOT E.. «El Derecho público de la crisis económica : transparencia y sector público» en AAVV (BLASCO ESTEVE, A.): *Hacia un nuevo derecho administrativo : actas del VI Congreso de la Asociación Española de Profesores de Derecho Administrativo,* Palma de Mallorca, 11 y 12 de febrero de 2011 , Madrid, 2012, págs. 283-387.

(71) ARRABAL PLATERO, P.: *La prueba tecnológica: aportación, práctica y valoración*, Valencia 2020, págs 168-172.

(72) GARCÍA MEXÍA, P.K., *Derechos y libertades, internet y tics*, Valencia, págs. 22 a 24.

(73) ARRABAL PLATERO, P: *La prueba tecnológica*., op.cit., pág. 171. En este sentido, la STS 426/2016, de 19 de mayo, establece que el acceso a los contenidos de cualquier ordenador por los agentes de policía « ha de contar con el presupuesto habilitante de una autorización judicial. […] Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal».

(74) GALLEGO SÁNCHEZ, E., «La patentabilidad de la inteligencia artificial. La patentabilidad de la inteligencia artificial. Otros sistemas de protección. En AAVV. (Dir. MUÑOZ PEREZ, A.F.), *Revolución digital, derecho mercantil y Token economía*., Madrid, 2019, pp. 239 – 270, pág. 276, señala que una vez Entrenados, los algoritmos son capaces de clasificar correctamente objetos que nunca han visto, en más y más casos con una precisión superior a la de los seres humanos. Por lo tanto, el acceso a los datos es un componente clave para un entorno competitivo de IA.

(75) Del mismo modo, la implementación efectiva de IA requiere la existencia de una conectividad reforzada a través de la coordinación del espectro, redes móviles 5G y fibras ópticas muy rápidas, nubes de próxima generación, así como tecnologías satelitales (Anexo a la Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones -Plan coordinado sobre la inteligencia artificial 7.12.2018, www.ipex.eu/IPEXL-WEB/dossier/files/./082dbcc5679fb7b40167a1b3f76300c1.do), ,

(76) Así, G´SELL F. «Les décisions algorithmiques», en AAVV. (dir. G´SELL F*) Le big data et le Droit*,,Paris 2020, págs..87-109, pág. 89.

(77) «Algorithms and human rigts». Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Committee of experts on Internet Intermdiaries (MSI_NET). Council of Europe Study DGY (2017) (12) Pág. 13. Disponible en: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

(78) Vid. Op.ult. cit., De forma muy gráfica, se indica quedo datos inocuos cuando se evalúan en comparación con un conjunto más grande de datos, pueden «reproducirse» y generar «baby data», cuya naturaleza puede ser completamente impredecible para el interesado. .

(79) Como recoge G´SELL F: «Les décisions algorithmiques, op.cit., pág. 98 se trata de «un lenguaje interior en un espacio propio dela máquina, que no tiene como función ser humanamente interpretable, pág. 98.

(80) BARRIO ANDRÉS, M., «Del derecho de internet al derecho de los robots» en AAVV (Dir. BARRIO ANDRÉS,M.): *Derecho de los robots*, Wolters Kluwer, Madrid 2018, págs.61-86, págs. 56-58.

(81) La narrow IA, que puede desarrollar tareas predefinidas. Vid. Al respecto, DILLON, C: AI: «Our Changing World», Patenting AI EPO Munich 30 May, 2018, disponible en https://e-courses.epo.org/course/view.php?id=151&lang=en,; SHEMTOV, N. «When Innovation Innovates: Assessing Inventive Step in Autonomous Inventive Processes», Patenting AI EPO Munich 30 May, 2018, disponible en https://e-courses.epo.org/course/view.php?id=151&lang=en. Sería el caso del Deep Blue de IBM, que solo juega al ajedrez.

(82) FLORES LÓPEZ,L./FERNÁNDEZ PERNÁNDEZ, H.M: *Las redes neuronales artificiales. Fundamentos teóricos y aplicaciones prácticas,* ed. Madrid, 2008, pág. 11.

(83) CLIFFORD, R.D. «Intellectual Property in the era of creative computer program: Wil the ture creator please stand up?, Tulane Law REview, 6(1991), pás. 1675-1703. Disponible en : https://scholarship.law.umassd.edu/cgi/viewcontent.cgi?article=1077&context=fac_pubs

(84) TUTT, A: «An FDA for algorithms», Administrative Law Review 83 (2017), ttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994, págs. 83-123, págs. 83 y ss.

(85) Pueden ser de tres tipos: el aprendizaje automático supervisado, que parte de datos ya «etiquetados»; el no supervisado , en el que no hay datos etiquetados por lo que se conocen cuáles son los datos de entrada, pero estos datos no se corresponden a un determinado *imput*, por lo que no existen, como tal, datos de salida. Este sistema puede plantear problemas de orden jurídico, como veremos. Finalmente, el aprendizaje autonómo por refuerzo, que es un sistema híbrido entre los dos anteriores. Vid. BARRIO ANDRÉS, M. ,» Del dercho de internet al derecho de los robots», op. cit, págs.. 60-66.

(86) Sus características esenciales son la especialización en un campo determinado (*expertise*), un amplio conocimiento de esa materia (*deepknowledge*), la utilización del razonamiento simbóbilo (*symbolic reasonig*) y la capacidad de autonocimiento que permite razonar sus decisiones (*self-knowledge*. Al respecto vid., E N N E S Z E/ YU-HSI N C H E N/ TIEN-JU YANG/ JOEL S. EMER:» Efficient Processing of)Deep Neural Networks: A Tutorial and Survey», Proceedings of the IEEE, 105 (2017), Disponible en https://ieeexplore.ieee.org/document/8114708, pág. 2296).

(87) BARRIO ANDRÉS, A: *Manual de Derecho Digital*, Valencia 2020, págs.62.

(88) SÁNCHEZ GARCÍA, L.: *El inventor artificial*, op.cit, pág. 43, citando a TURBAN, E./ARONSO,J.E./LIANGC, T.P., Decision suppor systems and intelligent systems, Neva Deli, 2007, pág. 550-551.

(89) BARRIO ANDRÉS, M., «Del derecho de internet al derecho de los robots», op.cit., pág. 70 y ss.

(90) GARCÍA-PRIETO CUESTA, J., ¿Qué es un robot» en AA.VV. Derecho de los robots (Dir. BARRIO Andrés, m.), Wolters Kluwer, Madrid 2018, PÁGS.25-59, pág.30.

(91) SÁNCHEZ GARCÍA, L.: *El inventor artificial*, op.cit., pág. 45.

(92) World Intellectual Property Organization (WIPO). WIPO Technology Trends 2019: Artificial Intelligence. Geneva: World Intellectual Property Organization., p. 143. Disponible en https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

(93) GALLEGO SÁNCHEZ, E., «La patentabilidad de la inteligencia artificial», op.cit., pág. 247 y ss.

(94) EPO-Guidelines2018- GII. 3.6, disponible en https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_6.htm).

(95) LIEVENS, K: «Patenting Artificial Intelligence», *Patenting AI EPO Munich 30 May, 2018*, disponible en https://e-courses.epo.org/course/view.php?id=151&lang=en).

(96) GALLEGO SÁNCHEZ, E. ,«La patentabilidad de la inteligencia artificial», op.cit., págs. 265-266.

(97) SAMUELSON, P.: «Privacy as intellectual property?», en *Standford Law review*, 52(2000), págs. 1125-1173, págs. 1157 y 1158.

(98) Este es el objetivo que inspira la European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI).

(99) Considerando K. Resolution on intellectual property rights for the development of artificial intelligence technologies

(100) Punto 10. Resolution on intellectual property rights for the development of artificial intelligence technologies

(101) Como se ha señalado, en medio del furor general por el sesgo algorítmico que describimos, «*cualquier remedio en una tormenta ha parecido atractivo». Vid.* EDWARDS, LILIAN/ VEALE, MI.:, «Slave to the Algorithm? Why a «Right to an Explanation» Is Probably Not the Remedy You Are Looking For (May 23, 2017). 16 *Duke Law & Technology Review 18 (2017),* págs. 18-84, pág. 82. Disponible en https://ssrn.com/abstract=2972855 or http://dx.doi.org/10.2139/ssrn.2972855

(102) Study on the human rights dimensions of automated data processing tecniques (in particular algorithms) and posible regulatory implications, pág. 15..

(103) EDWARDS, LILIAN/ VEALE, MI.:, «Slave to the Algorithm», op.cit.,, pág. 19

(104) Vid un exhaustivo comentario de este artículo en el trabajo de BYGRAVE, LEE. «Article 22. Automated individual decisión-making,including profiling en AA. VV.. ,págs. 522-542.

(105) Un comentario sobre el mismo, por ZANFIR-FORTUNA, G., Article 15. Right of Access by the data subject» en AAVV (Dir. KUNER,C/BYGRAVE,L/DICKSEY, C.); The EU General Data Protection REgulation (GDPR). A Commentary, Oxford 2020, págs. 449-468.

(106) Es un mecanismo al que se concede especial importancia a el UK GDPR cuyo artículo 25 establece: «*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures… and … integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects».*

(107) EDWARDS, LILIAN/ VEALE, MI.:, «Slave to the Algorithm? op.cit., pág. 82.

(108) Se alude a los «agentes inteligentes artificiales (AIA), como la categoría más evolucionada, capaz de percibir su entorno con sensores y de poder actuar. Vid. SANCHEZ GARCÍA, L., *El inventor artificial,* op.cit., págs. 68.

(109) Documento de sesión de 8.10.2020. A9-0186/2020. (2020/2012 (INL)). Con carácter previo, el Parlamento Europeo aprobó el 16 de febrero de 2017 una Resolución con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. Tal y como apunta el Parlamento, debe lograrse un marco jurídico adecuado a esta nueva realidad tecnológica. En las recomendaciones que efectúa a la Comisión para elaborar esa futura normativa, se debe tener especialmente en cuenta las implicaciones de orden ético y jurídico que el desarrollo de estos robots puede tener, entre otros ámbitos, en el de la protección de los datos personales.

(110) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL). tiene como objetivo generar confianza al proteger a los ciudadanos. El informe también busca promover la innovación y, al mismo tiempo, garantiza la seguridad jurídica a las empresas. En particular, se ha de tener presente la incidencia que cualquier tipo de regulación en este ámbito puede tener sobre las empresas emergentes y sobre las pymes. Por esta razón, una de las prioridades para el legislador europeo es que los desarrollos normativos introduzcan medidas proporcionadas que les permitan desarrollarse e innovar.

(111) Vid. SAN JUAN RODRÍGUEZ, N.: «La inteligencia artificial y la creación intelectual: ¿está la propiedad intelectual preparada para este nuevo reto?» (1), *La Ley Mercantil,* 72(2020), pags. 1-28.

(112) Recoge todas estas posturas SAN JUAN RODRÍGUEZ, N.: «La inteligencia artificial y la creación intelectual, op.cit., págs. 20 y ss.

(113) Así, NAVAS NAVARRO, S., «Obras generadas por algoritmos. En torno a su posible protección jurídica», RDC 2(2018), pág. 273-291, pág. 287.

(114) RAMALHO, A., «Ex Machine, Ex Auctore? Machines that créate and how Eu copyright law views them , disponible en Http://copyrghtblog.kluweiplaw.com/2018/11/12ex-machines´that´createánd´howéu´copyrighte-law´views-them/; SAN JUAN RODRÍGUEZ, N.: «La inteligencia artificial y la creación intelectual: ¿está la propiedad intelectual preparada para este nuevo reto? Op. .it, pág. 23

(115) Este Reglamento tiene como base tres importantes resoluciones del Parlamento europeo de 20 de octubre de 2020, con las que se pretende establecer las bases sobre cómo debería regularse en el ámbito de la Unión Europea la IA de modo que se permita impulsar la innovación, el respeto de estándares éticos y la confianza en la tecnología: Derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial; Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas; y, Régimen de responsabilidad civil en inteligencia artificial.

(116) Recogidas en el apartado 2.1. de la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones denominada «Generar confianza en la IA centrada en el ser humano». Bruselas, 8 de marzo de 2019. COM(2019) 168 final,

(117) 1) Acción y supervisión humanas Incluidos los derechos fundamentales, la acción humana y la supervisión humana. 2) Solidez técnica y seguridad Incluida la capacidad de resistencia a los ataques y la seguridad, un plan de repliegue y la seguridad general, precisión, fiabilidad y reproducibilidad. 3) Gestión de la privacidad y de los datos Incluido el respeto de la privacidad, la calidad y la integridad de los datos, así como el acceso a estos. 4) Transparencia Incluidas la trazabilidad, la explicabilidad y la comunicación. 5) Diversidad, no discriminación y equidad). Incluida la ausencia de sesgos injustos, la accesibilidad y el diseño universal, así como la participación de las partes interesadas. 6) Bienestar social y ambiental

Incluida la sostenibilidad y el respeto del medio ambiente, el impacto social, la sociedad y la democracia. 7) Rendición de cuentas Incluidas la auditabilidad, la minimización de efectos negativos y la notificación de estos, la búsqueda de equilibrios y las compensaciones.

(118) Señala el Consejo que *«En este contexto, para garantizar la compatibilidad de los sistemas automatizados con los derechos fundamentales y facilitar la aplicación de las normas jurídicas, deben afrontarse retos como la opacidad, la complejidad, el sesgo, cierto grado de imprevisibilidad y un comportamiento parcialmente autónomo. vista la complejidad, opacidad, sesgo y comportamiento de algunos sistemas de IA, que facilitara la aplicación de las normas jurídicas y garantizara el respeto de los derechos fundamentales»* (apartado 5). Consejo de la Unión Eiuropea, Conclusiones de la Presidencia- La carta de los Derechos Fundamentales en el contexto de la inteligencia artificicial u el cambio digital, Doc 11481/20, 2020. Disponible en : https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf

(119) Como es el caso de los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas. La legislación vigente en materia de protección de datos, protección de los consumidores y servicios digitales, que garantiza que las personas físicas sean debidamente informadas y puedan decidir libremente no ser sometidas a la elaboración de perfiles u otras prácticas que puedan afectar a su conducta, podría cubrir otras prácticas de manipulación o de explotación contra adultos que los sistemas de IA pueden facilitar. La propuesta prohíbe igualmente que las autoridades públicas realicen calificación social basada en IA con fines generales. Por último, también se prohíbe, salvo excepciones limitadas, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley.

(120) La transparencia es una de las Directrices para una IA fiable elaboradas por el grupo de expertos de alto nivel. La transparencia se identifica con «*la trazabilidad de los sistemas de IA; es importante registrar y documentar tanto las decisiones tomadas por los sistemas como la totalidad del proceso (incluida una descripción de la recogida y el etiquetado de datos, y una descripción del algoritmo utilizado) que dio lugar a las decisiones».*

(121) Se alude también a la *Diversidad, no discriminación y equidad;* señalando, que *«los conjuntos de datos utilizados por los sistemas de IA (tanto para el entrenamiento como para el funcionamiento) pueden verse afectados por la inclusión de sesgos históricos involuntarios, por no estar completos o por modelos de gobernanza deficientes. La persistencia en estos sesgos podría dar lugar a una discriminación (in)directa. También pueden producirse daños por la explotación intencionada de sesgos (del consumidor) o por una competencia desleal. Por otra parte, la forma en la que se desarrollan los sistemas de IA (por ejemplo, la forma en que está escrito el código de programación de un algoritmo) también puede estar sesgada. Estos problemas deben abordarse desde el inicio del desarrollo del sistema».*

(122) Una de las Directrices para lograr una IA fiable elaborada por el grupo de expertos *es la Privacidad y gestión de datos, considerando que «deben garantizarse la privacidad y la protección de datos en todas las fases del ciclo vital del sistema de IA. Los registros digitales del comportamiento humano pueden permitir que los sistemas de IA infieran no solo las preferencias, la edad y el sexo de las personas, sino también su orientación sexual o sus opiniones religiosas o políticas. Para que las personas puedan confiar en el tratamiento de datos, debe garantizarse que tienen el pleno control sobre sus propios datos, y que los datos que les conciernen no se utilizarán para perjudicarles o discriminarles».*

(123) La *Intervención y supervisión humana*» es otra de las Directrices para una IA fiable. Se trata de ayudar a las personas a elegir mejor y con más conocimiento de causa, apoyando los derechos fundamentales y no limitando o desorientando la autonomía humana.

(124) En las Directrices para lograr una IA fiable se estable que «*…la posibilidad de auditar los sistemas de IA es fundamental, puesto que la evaluación de los sistemas de IA por parte de auditores internos y externos, y la disponibilidad de los informes de evaluación, contribuye en gran medida a la fiabilidad de la tecnología. La posibilidad de realizar auditorías externas debe garantizarse especialmente en aplicaciones que afecten a los derechos fundamentales, por ejemplo, las aplicaciones críticas para la seguridad».*

(125) Se trata de introducir una serie de cambios en el Convenio 108 con la finalidad de: 1) abordar los desafíos a la intimidad derivados del uso de las tecnologías de la información y las telecomunicaciones; 2) reforzar el derecho a la protección de datos como derecho fundamental esencial para el ejercicio de otros derechos y libertades fundamentales en el tratamiento de datos personales; 3) conciliar el derecho a la protección de datos personales con el ejercicio de otros derechos y libertades fundamentales (especialmente la libertad de expresión); 4) reforzar los mecanismos de control del Convenio; 5) mantener el carácter general y tecnológicamente neutro de las disposiciones del Convenio; 6) preservar la coherencia y la compatibilidad del Convenio con otros marcos jurídicos aplicables, en particular el de la Unión Europea, y 7) preservar, reafirmar, reforzar y promover el alcance universal y el carácter abierto del Convenio 108. Committee on Legal Affairs and Human Rights Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Explanatory Report1.