RETOS DE LA DIGITALIZACIÓN PARA LA EMPRESA Y LOS CONSUMIDORES: ESTADO DE LA CUESTIÓN.

Nuria Fernández Pérez

Catedrática de Derecho Mercantil. Universidad de Alicante.

Codirectora del proyecto Análisis y seguimiento de los derechos digitales.

SUMARIO

IV. PROPIEDAD INTELECTUAL EN ENTORNOS DIGITALES
- 1. Consideraciones generales
- 2. Derecho de patentes.
  - 2.1. la patentabilidad de la inteligencia artificial
  - 2.2. Otras cuestiones problemáticas
- 3. El conflicto entre nombres de dominio y marcas
- 4. Los derechos de autor en el Mercado Único Digital.

V. LA INCIDENCIA DE LA INNOVACIÓN DIGITAL EN EL MERCADO FINANCIERO
- 1. Contexto
- 2. La aparición de las denominadas empresas fintech/insurtech
  - 2.1. Consideraciones generales
  - 2.2. .Régimen jurídico: problemas relacionados con el Derecho de la competencia y con la protección de los usuarios de servicios financieros
- 3. La aparición de nuevos productos y servicios financieros
  - 3.1 Nuevos sistemas y servicios de pago.
  - 3.2. El dinero digital: las cripto-monedas
  - 3.3. Neobanks y challenger banks
  - 3.4. Financiación participativa (crowdfunding). ICOs
  - 3.5. Asesoramiento y gestión de carteras.
  - 3.6. InsurTech

VI. INCIDENCIA DE LA DIGITALIZACIÓN EN EL FUNCIONAMIENTO DE LAS SOCIEDADES

I. EL ESTADO DE LA CUESTIÓN

1. La existencia de un nuevo contexto económico-social y, por tanto, jurídico

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. La economía mundial se está convirtiendo rápidamente en digital. El adjetivo digital en la vigesimosegunda edición del Diccionario de Lengua española de 2001, se refería a : "*perteneciente o relativo a los dedos, a los números dígitos y a una planta herbácea cuyas hojas se usan en medicina*". En la versión de 2019, se incluyen dos nuevas acepciones: "*dicho de un dispositivo o sistema: que crea, presenta, transporta o almacena información mediante una combinación de bits; y que se realiza o transmite por medios digitales"*. Las tecnologías de la información y la comunicación (TIC) no son un sector específico sino el fundamento de todos los sistemas económicos innovadores modernos, tal y como señala la Comisión Europea.

Tal y como se recoge con profusión en el informe *Digital Globalitation. The new era of global flows. (*March 2016. McKinsey Global I*nstitute)*, el mundo está más interconectado que nunca. Por primera vez en la historia, las economías emergentes son contrapartes. en más de la mitad de los flujos comerciales globales, y el comercio Sur-Sur es el tipo de conexión de más rápido crecimiento. Si bien los flujos de bienes y finanzas han perdido impulso, el ancho de banda transfronterizo utilizado ha crecido 45 veces más desde 2005, con una proyección de crecimiento hasta 2021 de nueve veces más. Las plataformas digitales han cambiado el modo en el que se realizan negocios entre particulares de diferentes países, reduciendo notablemente el costo de las transacciones, y creando mercados y comunidades de usuarios a nivel global. Las pequeñas empresas de todo el mundo se están convirtiendo en "micro-multinacionales" mediante el uso de plataformas digitales como eBay, Amazon, Facebook y Alibaba para conectarse con clientes y proveedores en otros países. Las empresas más pequeñas pueden nacer a nivel mundial

Por otra parte, nos encontramos con una suerte de nueva revolución industrial , la ya denominada Cuarta Revolución Industrial (4IR en sus siglas en inglés) que se está difundiendo a una velocidad sin precedentes al estar impulsada precisamente por medios digitales y tecnológicos. Internet no solo es un sistema de información colosal con acceso ilimitado y abierto a nivel mundial, sino también y de forma relevante una herramienta de interrelación social que excede la idea de mero canal de distribución comercial, y puede considerarse que está en el origen de un modelo revolucionario de funcionamiento de los mercados y de gestión de los negocios. Junto con internet, es preciso destacar como bases de esta última fase en la evolución económica, social, y por tanto jurídica en la que nos encontramos, las innovaciones en materia de inteligencia artificial y Big data, la computación distribuida como el registro distribuido o Blockchain, la criptografía, así como el propio acceso móvil a internet.

La denominada cuarta revolución industrial, 4IR, o industria 4.0., consiste en un fenómeno que, a grandes rasgos, hace referencia a la introducción de las tecnologías digitales en la industria concebida en sentido amplio. 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 Unico Digital de Europa. COM(2015) 192 FINAL). Hay una transición hacia fábricas y dispositivos "inteligentes" que operan de manera autónoma (European PAtent Office, Patents and the Fourth Industrial Revolution. The inventions behind digital transformation | December 2017, pág. 14.). 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 (Digital Globalitation. The new era of global flows. March 2016. McKinsey Global Institute).

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 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.

En la actualidad resulta evidente la existencia de un nuevo sustrato económico, pero también social, motivado por la expansión de las tecnologías de la información y comunicación. Es fácil advertir que si la forma de actuar de los diferentes operadores en el mercado está cambiando, porque el propio mercado también lo hace como consecuencia de la irrupción de la digitalización, el Ordenamiento Jurídico también debe contemplar ese nuevo escenario y atender las nuevas necesidades del tráfico económico.

La digitalización abre nuevas posibilidades al necesario crecimiento y permite la evolución de los modelos de negocio tradicionales, así como la aparición de nuevos modelos alternativos. El hecho de que no existan barreras de acceso para los proveedores de servicios de la sociedad de la información provoca la aparición de un nuevo escenario en la globalización de las empresas. Tal y como señala el Parlamento Europeo, la inteligencia artificial puede jugar un papel decisivo en la transformación digital de la sociedad. Su rápido avance dará lugar a más cambios en el trabajo, empresas y finanzas, sanidad, seguridad, agricultura y en muchos sectores. El grado de digitalización de la economía y de la sociedad y el uso de tecnologías digitales, influyen en los niveles de bienestar y desarrollo, así como en la productividad, la competitividad y la innovación;

teniendo importantes efectos en términos de crecimiento (CEOE, Plan Digital 2025. La digitalización de la sociedad española. Edición 20 noviembre de 2019). También se apunta como fundamental para el Pacto Verde Europeo y para la recuperación de la pandemia de COVID-19 (Noticias del Parlamento Europeo. Disponible en :https://www.europarl.europa.eu/news/es/headlines/society/20201015STO89417/regulacion-de-la-inteligencia-artificial-en-la-ue-la-propuesta-del-parlamento).

Para la Unión Europea, resulta imprescindible 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. Retos, riesgos y oportunidades de la sociedad digital. Tomas de la Quadra-Salcedo Fernández del Castillo, pags. 21-86

Nos encontramos en un momento en el que se obtiene por parte de las empresas una inmensa cantidad de datos, con el peligro de que esos datos son tratados para obtener informaciones diversas. Además, esos datos son proporcionados en ocasiones de forma consciente, pero en otras de forma inconsciente. 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 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. Es por ello, que resulta preciso contar con un marco jurídico adecuado para dar respuesta a la problemática jurídica anudada al mundo de los negocios digital.

Aunque se trata, como resulta obvio, de un fenómeno global y que, por tanto, incide en sectores muy diferenciados, lo cierto es que su repercusión es clara en los ámbitos propios de la regulación del Derecho Mercantil, tales como la contratación y negocios digitales, la propiedad intelectual, el Derecho de la competencia, el sector

financiero y el Derecho de Sociedades. Tanto por su origen (en el mercado) como por su aplicación (para el mercado), el Derecho Mercantil resulta de modo natural la vis atractiva de las normas que se han ido adaptando al entorno digital, así como de los nuevos desarrollos normativos dirigidos específicamente a regular nuevas realidades. De ahí, que podamos hablar de la construcción de un Derecho Mercantil Digital. Con todo, las consecuencias de esta transformación afectan prácticamente a todos los sectores del Ordenamiento Jurídico.

El conjunto de normas que abordan desde distintos prismas la penetración de la digitalización en nuestro mundo actual, al que de forma onmicomprensiva podría ya denominarse Derecho Digital se integra pues por aquellas normas que ex novo regulan aspectos que no tienen cabida en las disciplinas tradicionales y que cuentan con su propia regulación, lenguaje y elementos tecnológicos; como por aquellas otras que suponen una adaptación de esas disciplinas tradicionales para dar respuesta a los nuevos retos que plantea el entorno digital.

2. La digitalización del mercado: Nuevas herramientas de actuación

No es posible entender el proceso de digitalización sin hacer una referencia a los mecanismos que la propician. El Big Data y la inteligencia artificial son tecnologías esenciales en la transformación digital. A ellas se asocian otras como el internet de las cosas o la tecnología de registro distribuido. No se trata de hacer una descripción técnica, labor a la que se dedican los ingenieros; sino de conocer mínimamente su funcionamiento. Solo de este modo, se puede abordar su régimen jurídico.

En el proceso de digitalización que se extiende en el ámbito de los negocios nos encontramos, en efecto, con una auténtica revolución en el modo de capturar, procesar, analizar y visualizar los datos. 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. 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.

Por su parte, la inteligencia artificial *(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 (NAVAS NAVARRO, S. "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en AA. VV. Inteligencia artificial, Valencia, Tirant lo Blanch, 2017pág. 24) . 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- Inteligencia artificial 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 ((https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES*. Hay ámbitos, como el de la producción industrial o el del análisis de radiografías a través de ordenador donde los resultados son particularmente significativos (HOFFMAN-RIEM, W: Big Data. Desafíos también para el Derecho, Cizur Menor, Aranzadi, 2018, págs. 59 y ss).

Además, hablamos también de la denominada "machine learning", 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 problema*s (TUTT, A: "An FDA for algorithms", Administrative Law Review 83 (2017), ttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994, págs.. 1 y ss).*

Asimismo, debe destacarse como tendencia de cambio con repercusión en el mercado, el denominado Internet de las cosas (*Internet of Things,* IoT). Esta nueva potencialidad altera los modelos tradicionales de negocios y está dando lugar a otros nuevos sobre la base de la información que las empresas obtienen de objetos, conectados con sensores que facilitan información a tiempo real. De este modo, se automatizan tareas cotidianas y con ello se facilita la monitorización de los procesos, se optimiza las cadenas de suministro y conservación de los recursos. Todo ello con el fin lógico de mejorar la productividad de la empresa. Como señala la CEOE en su informe "Plan Digital 2025" (pág.25), se trata de "una gran oportunidad en plena evolución". Se piensa que podría llegar a haber 50.000 millones de dispositivos conectados al terminar el 2020, tanto en el ámbito de los coches (*conneted car*), del cuerpo (*Smart Health*), las ciudades (*Smart City*) y en otros sectores industriales. En esta evolución, los productos se transformación en servicios (la denominada Industria 4.0).

La mayoría de estas transformaciones parten de la aplicación de la inteligencia artificial () y de la tecnología de registro distribuido (*Distributed Ledger Technologies*, DLTs). Como su nombre indica se trata de una tecnología que permite mantener un registro digital de operaciones gracias a la validación que van realizando los participantes (nodos) de la red. El registro tiene forma de una cadena de bloques, en los que se agregan datos, que son firmados y validados digitalmente y que pueden proporcionar información precisa y desagregada de todos los detalles de las transacciones realizadas (intervinientes, fecha, hora, condiciones, etc.). Pueden ser de dos tipos: las centralizadas, que solo permiten a sujetos autorizados validar el registro digital de actuaciones; y las descentralizadas, que es el caso de la tecnología de la cadena de bloques (*Blockchain*) que resulta accesible por múltiples usuarios. La tecnología *Blockchain* parte, por tanto,

de la inexistencia de un registro centralizado que es sustituido por uno descentralizado con un número ilimitado de ordenadores conectados al sistema que valida los datos, dado que cada nodo de la red registra la operación.

Blockchain es por tanto una tecnología capaz de producir registros de información encriptados y encadenados –el contenido de un bloque solo puede descifrarse con la información del anterior- y que además quedan guardados en todos los nodos que componen la red. Así la información no se puede borrar ni modificar, es inalterable, porque cualquier cambio en un ordenador es detectado inmediatamente por el resto de partícipes. El registro centralizado se sustituye de este modo por uno descentralizado con un número ilimitado de ordenadores conectados al sistema que, valida los datos, dado que cada nodo de la red registra la operación. Se sustituye así la figura tradicional del tercero de confianza, que venía usándose en las transacciones electrónicas para dar seguridad y que es una figura central que cuenta con un régimen jurídico claro, por evidencias criptográfica; Estas redes, especialmente las descentralizadas, permiten reducir de forma notable los costes derivados de la intermediación. De ahí, su especial repercusión en todos los ámbitos, aunque con carácter especial en el sector financiero. La cuestión es determinar qué adaptaciones o nuevas normas se requieren para regular de forma satisfactoria este nuevo tipo de operatoria.

No se puede olvidar el carácter instrumental que la tecnología blockchain desempeña en el marco de la IA. Buen ejemplo de ello constituyen los smarts contracts, que constituyen una manifestación de la IA, cuya eficacia ha sido mejorada por la tecnología Blockchain. De ahí que aunque la expresión “smart contract” furae acuñada hace más de veinte años cuando apenas se estaba iniciando el boom de Internet, por Nick Szabo (informático, criptógrafo y jurista estadounidense), en un artículo publicado en el año 1996 en la revista Extropy con el título” Smart Contracts: Building Blocks for Digital Free Markets”, sea a partir de 2009 cuando comienza a tener un verdadero potencial.

La traducción literal del término Smart contrat sería el de contrato inteligente. Pero no puede hacerse esta traslación automática sin más. En primer lugar, porque la institución del contrato es un pilar esencial de nuestro sistema jurídico, que implica de

entrada, el acuerdo de voluntades (se entiende humanas).En cambio, nos encontramos con un programa de ordenador que se autoejecuta y hace cumplir por sí m ismo, de manera autónoma y automática, sin intermediarios, y por tanto, autoejecutable. Esto es posible al trasladar las cláusulas del contrato a códigos informáticos (scripts) que se auto ejecutarán cuando se produzca una situación predeterminada en el propio contrato. Esas situaciones predeterminadas o programas pueden ser de muy diferente tipo, desde efectuar pagos a emitir votos, etc. La virtualidad de estos contratos es que una vez que se establecen las circunstancias que van a dar lugar a la ejecución del contrato, no resulta posible ya establecer ningún tipo de modificación. Por tanto, las cláusulas que se establezcan (lo que se haya programado) son indisponibles en un momento posterior a la voluntad de las partes. Ello permite dotar de agilidad y sencillez a la contratación. A partir del primer smart contract, se podrán ir perfeccionando sucesivos contratos en cadena, en los que no será preciso ningún tipo de intervención humana. Por tanto, resulta una solución para el Internet de las cosas. En cuanto al adjetivo "smart" o "inteligente", como calificativo de este "contrato", parece dar a entender que habría graduación en los contratos. Esto no tiene sentido. Únicamente cabe entenderlo haciendo referencia a que se trata de una herramienta que se sustenta en inteligencia artificial.

3. Temas objeto de análisis

El objetivo del presente estudio es ofrecer una panorámica de la problemática que plantea la digitalización y de cómo pueden verse afectados los derechos de los ciudadanos, en su condición o no de consumidores. La irrupción de la digitalización trae consigo la necesidad de que el Derecho y la tecnología se interrelacionen. Incluso en el caso más simple, el de la máquina de vending, considera por Szabo como primer ejemplo de contrato de compraventa inteligente, donde los ingenieros informáticos ven secuencias programadas, los juristas ven un contrato. Y en el caso de que al introducir la moneda no salga el producto, donde esos ingenieros piensan en los códigos de error, los juristas se detienen en analizar de quien es la responsabilidad.

Se trata, por tanto, de determinar cuáles son las amenazas que plantea para el ciudadano la aparición de toda una serie de novedosos y variopintos productos, servicios y empresas. Con ello se está en condiciones de abordar en estudios posteriores, las soluciones jurídicas para que este nuevo contexto facilite una mayor productividad para las empresas, un mayor desarrollo económico y todo ello redunde en beneficio de los ciudadanos.

Para ello, debe analizarse con carácter general y previo, por su carácter transversal, la problemática que suscita el tratamiento de los datos y su incidencia sobre la esfera personal de los ciudadanos y sobre el desarrollo de la actividad empresarial.

La contratación a través de internet se ha convertido ya en algo usual para una buena parte de la población. Esto se ha puesto todavía más de manifiesto, a raíz de la crisis sanitaria generada por la Covid. En este ámbito, debe destacarse la contratación a través de plataformas de intermediación. Y las posibilidades de aplicación de los denominados contratos inteligentes (Smart contracts), como forma de evolución.

Por otra parte, no debemos olvidar que la digitalización se ha hecho especialmente patente en el sector financiero. Por ello, resulta esencial analizar cuáles son los nuevos productos y servicios en este ámbito y los mecanismos de tutela para el consumidor o usuario de productos y servicios financieros, sea en el ámbito bancario, del mercado de valores o del asegurativo.

Otro ámbito fundamental es la protección de los derechos de propiedad intelectual en el contexto digital. Si muchas de las innovaciones que sustentan la transformación digital se basan en nuevas herramientas y aplicaciones sustentadas en inteligencia artificial, resulta determinante y una de las primeras cuestiones a considerar, la determinación de cómo puede protegerse la innovación. Se trata de determinar qué tipos de innovaciones pueden ser patentadas y si hay otros métodos de protección jurídica. Igualmente, cómo afecta a la tutela de los derechos de marca la utilización generalizada de los nombres de dominio, o cómo incide la digitalización en los derechos de autor y conexos, son solo alguno de los aspectos a considerar.

Finalmente, también es clara la repercusión que sobre la creación, funcionamiento orgánico y modelo de negocio de las sociedades pueden tener las tecnologías digitales, especialmente por su importancia en el tejido empresarial de la provincia de Alicante, para las pymes y las empresas familiares.

Todas estas cuestiones merecen un tratamiento particularizado que será objeto de futuros estudios. Y además, se complementan necesariamente, con el análisis de la incidencia de la digitalización en la esfera de los derechos fundamentales de los ciudadanos. No en vano, entre esos derechos se encuentra el derecho a la protección de datos, el derecho a la libertad de empresa y a la protección de las personas consumidoras y usuarias en un entorno digital.

II. PROBLEMÁTICA GENERAL: COLISIÓN ENTRE PROTECCIÓN DE DATOS Y DESARROLLO EMPRESARIAL.

1. La economía de los datos

La globalización y el desarrollo tecnológico han planteado nuevos retos para la protección de los datos personales. La tecnología proporciona en la actualidad potentes instrumentos de captación y de intercambio de datos en unos volúmenes cada vez más crecientes y sin precedentes. Resulta cada vez más habitual la difusión por parte de las personas físicas de un importante volumen de datos personales. Aunque Europa todavía se encuentra en una posición más menos consolidada con relación a las aplicaciones de consumidores y las plataformas en línea (lo que se traduce en una desventaja competitiva en el acceso a los datos), se están experimentando cambios importantes en el valor y la reutilización de los datos en los distintos sectores. El volumen de datos producido en el mundo va en aumento rápidamente. Las cifras previstas para 2025 son realmente sorprendentes: un 530% de incremento del volumen global de datos (de 33 zetabytes en 2018 a 175 zetabytes), 829.000 millones de euros el valor de la economía de los datos, 10,9 millones de profesionales de los datos (Datos recogidos por la Comisión Europea

en la Estrategia europea de datos. Hacer de la UE un modelo de sociedad capacitada por los datos.

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 que prestan servicios como titulares de redes sociales, buscadores o servicios de compra muy extendidos en la actualidad. La aplicación de programas de inteligencia artificial 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 para ella adelantándose a cualquier competidor o entrando en nuevos mercados (DE LA QUADRA SALCEDO, T., "Retos, riesgos y oportunidades de la sociedad digital", AAVV. Sociedad Digital y Derecho, 2018. pág. 45).

El Big Data y su tratamiento supone un salto cualitativo muy portante que coloca a quien dispone de los datos y del conocimiento y técnicas para tratarlos en una situación de ventaja competitiva sin precedentes (Pasquale, Frank «The black Box Society: The Secret Algorithms that control Money and information» Ed. Cambridge: Harvard University Press, 2015), 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.

Hay que tener en cuenta que se produce una concentración asimétrica de conocimientos en muy pocos actores, lo que exige aplicar unas normas, no muy diferentes a las que en la actualidad se ocupan de la defensa de la competencia, pero sí adaptadas a este nuevo escenario. Deben tenerse además en consideración aspectos muy importantes relativos al modo de acceso de los datos, el carácter gratuito o no del consentimiento

prestado, su carácter anónimo, etc. La creación de perfiles digitales pueden tener algunos efectos positivos, como la personalización en la oferta de productos y servicios, pero también lógicamente pueden suponer una amenaza para la privacidad de la persona, al permitir obtener información sobre los hábitos gustos y modo de vida de las personas, sin que sean conscientes de ellos. Además, pueden constituir también la vía para que hackers puedan a través de dispositivos conectados invadir virtualmente el espacio donde están los aparatos conectados (sea la casa, la oficina, el coche etc).

El tratamiento de los datos, y el internet de las cosas plantea más que nunca la existencia de un conflicto entre información y privacidad; entre protección de datos y desarrollo empresarial. En 2014 las Autoridades europeas de protección de datos aprobaron el primer Dictamen conjunto sobre internet de las cosas. El documento, cuya elaboración fue liderada por la Agencia Española de Protección de Datos junto con la Autoridad francesa (CNIL), acoge con satisfacción las perspectivas de beneficios económicos y sociales que puede suponer esta tecnología, pero también identifica y alerta de los riesgos que estos productos y servicios emergentes pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades

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.

En el fondo hay un importante problema derivado por el modo radicalmente distinto en el que se protegen los datos personales en el ámbito de la Unión Europea -que se expone en el apartado siguiente-, y en Estados Unidos. En la Unión Europea, gozamos de un marco legal garantista, caracterizado por su carácter reglado. En Estados Unidos, no se dispone de una legislación federal. Únicamente en algún estado como California, se cuenta con una norma al respecto., 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. También establece que hay normas al respecto. 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.

2. La normativa europea y española en materia de protección de datos: un punto de partida.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. Viene recogido en el ámbito europeo en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) que establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le concierna. Y en nuestro país, en el artículo 18.4 CE. A estos efectos, resulta de particular interés la Comunicación de la Comisión, acerca de una "Estrategia europea de datos. Hacer de la UE un modelo de sociedad capacitada para los datos" en la que se establece:

> *"En los últimos años, las tecnologías digitales han transformado nuestra economía y nuestra sociedad, afectando a todos los sectores de actividad y a la vida diaria de todos los europeos. Los datos están en el centro de esta transformación, y va a ir a más. La innovación basada en los datos reportará enormes beneficios a los ciudadanos, por ejemplo, mediante la mejora de la medicina personalizada, la nueva movilidad y su contribución al Pacto Verde Europeo. En una sociedad en la que las personas generarán cantidades cada vez mayores de datos, la manera en que se recogen y utilicen los datos debe situar los*

intereses de la persona en primer lugar, de conformidad con los valores, los derechos fundamentales y las normas europeos. Los ciudadanos solo confiarán y harán suyas las innovaciones basadas en los datos si confían en que todo intercambio de datos personales en la UE estará sujeto al pleno respeto de sus estrictas normas en materia de protección de datos".

Este nuevo contexto es el que ha motivado una profunda revisión de la normativa de la Unión Europea, al objeto de reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas. De este modo, además, es como se puede generar la confianza necesaria para que la economía digital pueda desarrollarse en todo el mercado interior. En este entorno digital dominado por la tecnología de Big Data y por el almacenamiento de datos en la nube (*cloud*), aparecen nuevos problemas relacionados con el derecho al olvido y nuevas formas de delincuencia asociadas a la identidad digital.

Son significativas a este respecto las palabras de la Comisión Europea (Estrategia Europea de Datos, pág. 5) "*La visión de la Comisión se deriva de los valores y derechos fundamentales europeos y de la convicción de que el ser humano es y debe seguir siendo lo más importante. La Comisión está convencida de que el uso de los datos puede dar a las empresas y el sector público de la UE los medios para tomar mejores decisiones. Es tanto más imperativo aprovechar la oportunidad que presentan los datos relativos al bien social y económico cuanto que, a diferencia de la mayoría de los recursos económicos, los datos pueden replicarse a un coste próximo a cero y su utilización por una persona u organización no impide la utilización simultánea por otra persona u organización. Este potencial debe ponerse en práctica para abordar las necesidades de las personas y crear así un valor para la economía y la sociedad. Si se quiere liberar tal potencial, es necesario garantizar un mejor acceso a los datos y su uso responsable*"

En esta línea se han aprobado dos importantes normas que componen lo que se conoce como el nuevo marco europeo de protección de datos y que deben ser de especial aplicación respecto de las empresas que usan tecnología Big data: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la

protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) y la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. El RGPD unifica y moderniza la normativa europea sobre protección de datos, estableciendo mecanismos para que, por un lado, los ciudadanos puedan tener un mejor control de sus datos personales y por otro, las empresas puedan aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores. En lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, apela a la "privacidad por diseño", para que la protección de datos se tenga en cuenta desde el principio en el diseño mismo de las aplicaciones.

La Directiva de Protección de Datos, por su parte, está destinada a la protección de los datos de víctimas, testigos y sospechosos de la comisión de delitos en los ámbitos policiales y de la Justicia. Las personas físicas deben tener el control de sus propios datos personales.

Siguiendo esa estela, se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD). Teniendo que cuenta que el RGPD es de aplicación directa, cabría hablar de desarrollo o complemento del Derecho de la Unión Europea, tal y como establece la Exposición de Motivos de la LOPD. Por tanto, en materia de protección de datos habrá que aplicar ambas disposiciones. El campo para nuestra norma será organizativo y de completar aquellos elementos que no hayan sido desarrollados en la norma comunitaria. En ese sentido, la ley matiza y completa el régimen del RGPD en cuanto a los principios básicos de tratamiento de datos. Exactitud, confidencialidad, consentimiento son los que han de seguirse por parte de los encargados y responsables. Estas reglas, que son las que abren la puerta a los derechos que reconoce la ley en relación con los datos, están modulados

en una serie de supuestos específicos que atañen directamente al ámbito mercantil: tratamiento de datos de con-tacto de empresarios individuales y de profesionales liberales (art. 19), sistemas de información crediticia, (art.20), tratamientos relacionados con la realización de determinadas operaciones mercantiles (art. 21) y sistemas de exclusión publicitaria (art. 23).

En relación con el régimen de exclusión publicitaria, el artículo 23 LOPD, establece una serie de prescripciones. En primer lugar, que será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. En este sentido, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a las personas a las que se dirigen, a las que la ley denomina afectados. Es posible, además, que los interesados establezcan únicamente limitaciones a la recepción de comunicaciones comerciales de determinadas empresas.

En segundo término, establece que quienes deseen utilizar los datos personales para la remisión de comunicaciones comerciales deberán informar a los afectados acerca de los sistemas de exclusión publicitaria existentes. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias. La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

Finalmente, señala que quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. No será necesario realizar esa consulta cuando el afectado, siguiendo lo establecido en la ley,

hubiera prestado su consentimiento para recibir la comunicación a quien pretenda realizarla.

Siendo significativos los avances producidos con esta normativa, son todavía muchos los aspectos a tener en cuenta, y que dependen también de los concretos sectores en los que se realice el acceso de los datos.

III. DERECHOS DE LOS CONSUMIDORES EN LA CONTRATACIÓN ELECTRÓNICA. LA CONTRATACIÓN MEDIANTE PLATAFORMAS. EL CASO PARTICULAR DE LOS SMART CONTRACTS.

1. La generalización de la contratación electrónica

1.1. La contratación electrónica: marco jurídico

La contratación electrónica constituye, sin duda, un fenómeno en plena expansión, que ha venido a alterar el modo tradicional de contratar, no ya sólo en la contratación entre presentes, sino en los contratos a distancia. El 72% de los usuarios de internet en España entre 16 y 70 años utiliza esta vía para realizar sus compras, lo que se traduce en 22,5 millones de personas. Estos datos extraídos del VII Estudio Anual de Ecommerce en España 2020, evidencian el auge y la importancia en términos cuantitativos del comercio on line.

Frente a las vías tradicionales cuyo común denominador es que tienen como soporte la distribución escrita o la vía postal, este tipo de contratación que se desarrolla al amparo del comercio electrónico, se caracteriza por desarrollarse a través de medios telemáticos y redes de telecomunicación. Como nuevo soporte del intercambio de bienes y servicios, estos medios vienen sustituyendo, de forma cada vez más generalizada, a los medios clásicos para la emisión y recepción de voluntades con eficacia negocial, lo que da lugar a un nuevo ámbito de ejercicio de la actividad mercantil, una suerte de mercados virtuales.

Como todos los cambios en el Derecho en general y, en el Derecho Mercantil en particular, tiene por finalidad fomentar y agilizar la consecución de transacciones comerciales adaptándose a la realidad económica. No obstante, la desmaterialización del documento y del propio mercado en el que se produce la operatoria da lugar a una importante problemática de carácter pluridisciplinar y por tanto, plantea importantes retos al Ordenamiento Jurídico.

La contratación electrónica, independientemente del objeto sobre el que recaiga, plantea la dificultad de aplicar conceptos y categorías jurídicas tradicionales a contratos en los que concurren las características de desmaterialización anteriormente apuntadas. Además, y como consecuencia directa del desarrollo del comercio electrónico y de la penetración de las tecnologías de la información en todos los ámbitos de la economía, los mercados nacionales como tales pueden considerarse que han sido ampliamente superados.

Dada, por otra parte, la rapidez con la que se producen los avances tecnológicos que inciden de forma directa en el modo de contratación, no parece aconsejable mantener un concepto estricto de contrato electrónico como se venía haciendo, en el que únicamente se tome en consideración el hecho de que la perfección del contrato se produzca mediante el intercambio electrónico de datos de ordenador a ordenador, ya sea a través de las aplicaciones de internet, como máximo exponente de redes abiertas de telecomunicación, básicamente el correo electrónico o el Word Wide Web; ya sea a través del sistema EDI (Electronic Data Interchange), caracterizado porque su uso se encuentra restringido a quienes están oportunamente habilitados. En todo caso, admitida en la actualidad sin fisuras la validez y eficacia de los contratos electrónicos, continúan surgiendo cuestiones a abordar como las relativas a la perfección de los contratos, a la prueba de los mismos o a la eventual falta de seguridad en las transacciones electrónicas. En efecto, entre los consumidores se constata la preocupación por aspectos que pueden parecer básicos en la contratación tradicional, pero que asumen fundamental importancia cuando se realiza por estos medios, máxime a través de redes abiertas como Internet, tales como asegurar la identidad de los intervinientes, la integridad y la confidencialidad del

mensaje. Podría apuntarse finalmente otros aspectos de relevancia como la propia seguridad del pago electrónico, la asunción de responsabilidad en casos de conflicto, así como los riesgos de potenciales abusos que el uso de los medios telemáticos puede originar (transferencias fraudulentas de fondos...) etc. Asimismo, hay que considerar que, tratándose en muchas ocasiones de operaciones de carácter transfronterizo, surge el problema de coordinar las distintas legislaciones, máxime cuando en la contratación intervienen consumidores que cuentan con específicas medidas de tutela en cada país. Especial complejidad se produce cuando el objeto de la transacción son contenidos o servicios digitales.

Todos estos problemas se agravan en el caso particular de los smarts contracts, que precisan no solo una adaptación de las normas tradicionales sino posiblemente nuevos planteamientos jurídicos.

En la actualidad resulta pertinente aludir a un concepto amplio de contrato electrónico entendiendo por tal aquel que permite la realización de un negocio jurídico utilizando un sistema electrónico, por lo que quedarían comprendidos en su noción los contratos celebrados a través de vías que pueden ya considerarse tradicionales; y además, a través de otras derivadas de la irrupción veloz de tecnologías como el Blockchain que están en la base de un nuevo tipo de contratos sin intervención humana, los denominados *smarts contracts.*

Su disciplina se encuentra, en primer término, en la Ley de Servicios de la Sociedad dela Información y comercio electrónico (LSSICE), que, no obstante, excluye de su ámbito de aplicación a los contratos relativos al Derecho de familia y sucesiones. Asimismo, los actos o contratos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica (art. 23.4 LSSICE). No se contempla tampoco ninguna disposición aplicable a los smarts contracts o a otro tipo de contratos basados en tecnología blockchain, teniendo en cuenta lo reciente de su irrupción en el tráfico mercantil.

Cuando estos contratos estén firmados electrónicamente se estará a lo establecido la Ley 59/2003, de 19 de diciembre, de firma electrónica. Adicionalmente, los contratos electrónicos se regirán por lo dispuesto en los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial (art. 23.1 LSSICE). Por consiguiente, si el adquirente del bien, o el receptor del servicio, es un consumidor resulta aplicable el TRLCU. En particular las normas sobre contratación a distancia. No puede dudarse, en efecto, de que la contratación electrónica es un tipo de contratación a distancia, como prevé expresamente el art. 94 TRLCU. Conforme a este texto legal, cuando exista contradicción entre las previsiones del mismo y la LSSICE, prevalecerá esta última, salvo en materia de información precontractual en la que serán preferentes las normas del TRLCU (arts. 94 y 97.7 TRLCU). Hay que tener en cuenta también que la comercialización a distancia de los servicios financieros destinados a los consumidores se rige por una Ley especial, la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores.

1.2.Derechos que asisten a los consumidores

1.2.1. Régimen de información precontractual

La protección se articula básicamente a través de un régimen de información precontractual previa, la regulación de las comunicaciones comerciales, y aspectos relativos a la ejecución del contrato, donde juega un papel esencial el derecho de desestimiento.

Salvo que ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o cuando el contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente (art. 27. LSSICE), el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tiene la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante

técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los extremos consignados en la LSSICE, entre los que destacan, los trámites que deben seguirse para celebrar el contrato y los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos; así como las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Estas obligaciones se darán por cumplidas si el prestador incluye los datos anteriores en su página o sitio de Internet en las condiciones señaladas antes. Sin embargo, en caso de que el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, cuando se facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario (art. 27.1 LSSICE). Adicionalmente, sienta el principio de que, siempre que la Ley exija que el contrato, o cualquier información relacionada con el mismo, conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico (art. 23.3 LSSICE).

Por otra parte, la ley prohíbe prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que, previamente no hubieran sido solicitadas, o expresamente autorizadas, por los destinatarios de las mismas, salvo que exista una relación contractual previa y siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales y de revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales mediante un procedimiento sencillo y gratuito. Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio

deberá consistir necesariamente en la inclusión de una dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección (arts. 21 y 22 LSSICE).

A estos efectos se ordena que las comunicaciones comerciales realizadas por vía electrónica sean claramente identificables como tales y que también lo sea la persona física o jurídica en nombre de la cual se realizan, prohibiendo en todo caso el envío de aquellas en las que se disimule o se oculte la identidad de este último. Y en los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, se deberá asegurar, además, el cumplimiento de las normas de ordenación del comercio, que queden claramente identificadas como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca (art. 20 LSSICE). Por otra parte, la aplicación de estas normas procede junto con las previstas en su disciplina propia, la vigente en materia comercial y de publicidad y con la LPD (art. 19 LSSICE).

1.2.2. Oferta, consentimiento y derecho de desistimiento.

La LSSICE obliga a mantener la oferta durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezca accesible a los destinatarios del servicio (art. 27.3 LSSICE). Por otra parte, en materia de perfección del contrato, reproduce la regla general de perfección del contrato por el consentimiento, advirtiendo que, para su validez, no es necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos. La concurrencia del mismo se determina con los criterios previstos para la contratación entre ausentes, por ser la electrónica una modalidad de este tipo (art. 54 Ccom), pero la LSSICE le somete a una disciplina adicional. En primer término, salvo los casos expresamente previstos en la LSSICE (art. 28.3 LSSICE), obliga al oferente a confirmar la recepción de la aceptación por los medios que relaciona (art. 28.1 LSSICE), aunque se entiende que se ha recibido cuando el oferente al que se dirija pueda tener constancia de ello (art. 28.2 LSSICE). Por otra parte, en el caso de que la

recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario pue-de tener constancia de la confirmación desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utiliza-do para la recepción de comunicaciones (art. 28.2 LSSICE).

El derecho de desisimiento otorga al consumidor la facultad de dejar sin efecto el contrato celebrado, sin necesidad de justificar su decisión, con el único requisito de notificárselo así a la otra parte contratante, en el plazo de 14 días naturales desde la recepción del bien objeto del contrato o desde la celebración de éste si el objeto del contrato fuera la prestación de servicios El ejercicio del derecho no está sujeto a formalidad alguna, bastando que se acredite en cualquier forma admitida en derecho. En todo caso se considerará válidamente ejercitado mediante el envío del documento de desistimiento, que, necesaria-mente, deberá entrega el empresario, o mediante la devolución de los productos recibidos (arts. 69 y 70 TRLCU). Si la comunicación se remite electrónicamente, el empresario comunicará sin demora al consumidor en un soporte duradero el acuse de recibo de dicho desistimiento (art. 106.3 TRLCU). Por lo demás, dicha comunicación ha de enviarse antes de que finalice el plazo de ejercicio del derecho (art. 106.2 TRLCU).

En cuanto a los efectos del ejercicio del derecho, el consumidor sólo será responsable de la disminución de valor de los bienes resultante de una manipulación de los mismos distinta a la necesaria para establecer su naturaleza, sus características o su funcionamiento. En ningún caso será responsable de la disminución de valor de los bienes si el empresario no le ha informado de su derecho de desistimiento (art. 108.2 TRLCU). En este mismo contexto, al deber del empresario de devolver el precio se añade el de reintegrar también los costes de entrega. No obstante, como excepción al principio aplicable en el régimen común conforme al cual el ejercicio del derecho de desistimiento no implicará gasto alguno para el consumidor (art. 73 TRLCU), en este tipo de contratos, si el consumidor ha seleccionado expresamente una modalidad de entrega diferente a la modalidad menos costosa de entrega ordinaria, el empresario no estará obligado a reembolsar los costes adicionales que de ello se deriven (art. 107.2 TRLCU). Y sólo

soportará los costes directos de devolución de los bienes, salvo si el empresario ha aceptado asumirlos o no le ha informado de que le corresponde asumir esos costes (art. 108.1 TRLCU). Adicionalmente, a menos que el empresario se haya ofrecido a recoger él mismo los bienes, en los contratos de venta, el empresario podrá retener el reembolso hasta haber recibido los bienes, o hasta que el consumidor haya presentado una prueba de la devolución de los mismos, según qué condición se cumpla primero (art. 107.3 TRLCU).

1.3. Problemas específicos derivados de procesos automatizados basados en Inteligencia artificial.

Tal y como se ha puesto de manifiesto, el problema relativo a la protección de los datos y a la creación de perfiles digitales tiene carácter transversal. En este sentido, el comité del mercado interior y protección de los consumidores emitió una Resolución con fecha 21-01- 2020 (Draft motion for a resolution further to Question for Oral Answer B9- /2019 pursuant to Rule 136(5) of the Rules of Procedure on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services (2019/2915(RSP)). La idea central que subyace es la necesidad de que el consumidor esté informado de cuando se está utilizando servicios digitales, tales como asistentes virtuales y chatbots; y cuando están interactuando con estos sistemas de decisión autónoma, Deben conocer cómo funcionan y como pueden corregirse y chequearse las decisiones adoptadas por esos sistemas. Es preciso que los empresarios informen a los consumidores cuando los precios de los bienes o los servicios se están ofertando de forma personalizado utilizando sistemas de IA que analizan el comportamiento del consumidor, sus gustos y hasta su poder adquisitivo. Incluso que pueden llegar a discriminar a consumidores teniendo en cuenta su lugar de residencia, nacionalidad. Revisión Directiva 2019/2161 y Reglamento 2018/302

Por otra parte, también hay que tener en cuenta que se están utilizando sistemas de IA para resolver de modo alternativo (sistemas ADR) controversias entre empresarios

y consumidores. De ahí , que en una futura revisión de la Directiva 2013/11 sobre resolución alternativa de litigios de consumo y el Reglamento UE 524/2013 sobre resolución de litigios en línea para litigios de consumo, se tengan en cuenta estas cuestiones. De hecho, en nuestro país, la AEPD está promoviendo un sistema extrajudicial (ADR) de conflictos que aligere y abarate para la ciudadanía la protección de sus derechos en materia de protección de datos.

Otro tema importante es el relativo a la responsabilidad civil derivada de un producto defectuoso implementado con un sistema de inteligencia artificial. El hecho de que los productos puedan adoptar decisiones automatizas y que puedan evolucionar en su toma de decisiones y adoptar decisiones no previstas inicialmente plantea un gran interrogante.Todos los que intervienen en el proceso deben tener claro cuál es el régimen jurídico que se les va aplicar y su responsabilidad sobre el resultado final. Conceptos como daño, defecto o responsabilidad van a tener que sufrir una revisión. Es muy importante, además, que en el seno de la Unión Europea se logre armonizar este aspecto, del que depende en última instancia el propio desarrollo del sector.

En los casos en los que pueden verse afectados intereses públicos, debe poder constatarse supervisarse por profesionales cualificados.

2. Contratación mediante plataformas digitales: aspectos problemáticos relacionados con los intermediarios.

2.1. La intervención de plataformas como elemento definitorio de la economía de plataforma

Además de los negocios tradicionales, realizados ahora por vía electrónica y a los que se hacía referencia con anterioridad, el imparable desarrollo de las tecnologías de la comunicación ha sido un acicate en la aparición de nuevos modelos de negocio. La explicación es sencilla: cada vez resulta más fácil la transmisión de información y la

comunicación de las partes; por otra parte, además del uso generalizado de internet, los ordenadores cada vez permiten más funcionalidades y tienen mayor potencia, lo que permite automatizar de forma más sencilla las operaciones, así como la proliferación entre la población de terminales móviles inteligentes. Y como resulta evidente, el hecho de que se pueda acceder a información y contratar un servicio en cualquier lugar y momento, aumenta las posibilidades de que esto se lleve a cabo.

Nos encontramos, por tanto, con la suma de dos ingredientes, que han dado lugar a la aparición de nuevos negocios con intervención de nuevos prestadores de servicios de la sociedad de la información, dentro de un contexto que se ha venido a denominar como Economía colaborativa, por más que se trate de un concepto de perfiles muy ambiguos que permite aludir a fenómenos muy diversos y que comienza a ser sustituido por el de Economía de Plataforma o Economía Circular 2.0.

Las plataformas aparecen como un eje central de este nuevo tipo de actividad, que en la mayoría de las ocasiones, constituye una auténtica actividad empresarial. Aunque ese tipo de plataformas existían con anterioridad a que se comenzara a hablar del fenómeno de la economía colaborativa, lo que diferencia el nuevo modelo es que las plataformas actúan en mercados multilaterales mientras que antes lo hacían en mercados bilaterales; esta circunstancia conlleva la existencia de prestadores más descentralizados, que no tienen por qué ser necesariamente profesionales, que utilizan una plataforma para que medie en la contratación de sus servicios o productos por terceros.

Este nuevo modelo implica un nuevo contexto de competencia y el establecimiento de nuevas relaciones a través de la creación de valor en la cadena de suministro (proveedores, productores, distribuidores y consumidores). No hay un único modelo, en la medida que uno de los elementos que conforman este nuevo escenario, las plataformas digitales, presentan múltiples variantes. Cubren una amplia gama de actividades, entre las que se incluyen motores de búsqueda, plataformas de publicidad, redes sociales y medios de difusión de contenidos, servicios de comunicación, plataformas de distribución de aplicaciones, sistemas de pago y plataformas de financiación participativa, por citar solo algunos ejemplos. De ahí, que comience a

asentarse, como se ha indicado, el término de economía de plataforma o economía circular 2.0, por ser términos que engloban mejor la distinta fenomenología de las actividades llevadas a cabo a través de las plataformas digitales.

Con todo, como señala la Comisión Europea en su Comunicación "*Las plataformas en línea y el mercado único digital. Retos y oportunidades para Europa*" las diferentes plataformas cuentan con una serie de características comunes, que nos resultan útiles para perfilar los contornos de este nuevo modelo de actividad económica:

i) "Tienen capacidad para crear y modelar nuevos mercados", con lo que se convierten en un potente competidor para los mercados tradicionales, planteándoles el desafío de su adaptación; además, se convierten en instrumentos óptimos para organizar nuevas formas de participación o para efectuar en línea negocios consistentes en la recogida, tratamiento y edición de grandes cantidades de datos.

ii) "Actúan en mercados plurifacéticos", y lo hacen dependiendo del modelo concreto, con diferentes grados de control sobre las interacciones directas entre grupos de usuarios.

iii) Se benefician de los "efectos de red", lo que significa en sentido amplio que el valor del servicio aumenta con el número de usuarios.

iv) De forma bastante generalizada, se apoyan en las tecnologías de la información y la comunicación para llegar a sus usuarios de forma instantánea y sin esfuerzo.

v) Su papel es esencial en la creación de "valor digital", por ejemplo, mediante la acumulación de datos o facilitando nuevos proyectos empresariales

2.2. La existencia de diferentes modelos de plataformas y su problemática jurídica

Este modelo de actuación que gira en torno a plataformas digitales, como es obvio, resulta un fenómeno global y transversal, que ha propiciado la aparición de starts up para compartir los más variopintos servicios o cosas. Así, desde las más comunes, como son las de compartir trayectos de coche o el propio coche o la vivienda, nos encontramos otras de crowdfunding, o para intercambiar productos, para comprar y vender muebles de segunda mano etc. También al amparo de estas prácticas han surgido plataformas tecnológicas que ponen en contacto a los oferentes y demandantes, llegando a convertirse en importantes empresas por el volumen de negocio que realizan, como es el caso por ejemplo de Airbnb en el sector del alojamiento o de Uber en el del transporte.

La cuestión con todo y con carácter general, cuando hablamos de este modelo de economía de plataforma, es delimitar si nos encontramos con negocios entre particulares, entre los cuales la función de las plataformas es meramente la de un servicio de la sociedad de la información, lo que eliminaría los problemas relacionados con el Derecho de la Competencia; o por el contrario, actúan como empresarios, teniendo en cuenta el concepto jurídico que del mismo proporciona el Derecho Mercantil, lo que determina la aplicación de un régimen más restrictivo, incluida la normativa de protección a los consumidores, así como aspectos relacionados con el Derecho de la Competencia.

Por otra parte, es esencial determinar cuál es la función que realizan los prestadores de servicios de la sociedad de la información. La principal consecuencia para una plataforma de su consideración como tal es la aplicación de dos principios fundamentales recogidos en la Directiva sobre servicios de la sociedad de la información y comercio electrónico y recogidos en nuestra Ley de servicios de la sociedad de la información y comercio electrónico: el de libre prestación de servicios, que implica la ausencia de autorizaciones para el ejercicio de la actividad; y el de neutralidad tecnológica, que está directamente relacionado con el régimen de responsabilidad. La

regla general es que los prestadores de los servicios de la sociedad de la información únicamente serán responsables por los contenidos que ellos mismos u otros por cuenta suya, hayan elaborado. Tanto la Directiva como la norma española establecen un sistema de exención de responsabilidad por daños y perjuicios respecto de contenidos ilícitos, cuando los prestadores lleven a cabo una de las funciones de intermediación técnica previstas - es decir, cuando operen como proveedores de la técnica de comunicación-. No serán, por tanto, responsables por los contenidos ajenos que, en el ejercicio de tales funciones, transmitan, copien, almacenen o localicen (arts. 13 a 17 LSICE).

El problema es que en la actualidad esos prestadores de servicios de la sociedad de la información han evolucionado y en numerosas ocasiones realizan funciones que exceden propiamente de las que vienen configuradas legalmente, actuando como intermediarios entre los prestadores de los servicios subyacentes (por ejemplo, el transporte o el alojamiento) y sus usuarios. En particular, en determinadas circunstancias, una plataforma puede ser también un proveedor del servicio subyacente; es el caso de la plataforma Uber que ha sido considerada por el TJUE como una auténtica empresa de transporte y no como un prestador de servicios de la sociedad de la información, lo que implica que dejen de tener aplicación los principios anteriormente señalados.

El problema, no resuelto aún, está en las plataformas que excediendo las funciones propias de un prestador de servicios de la sociedad de la información (como es el caso típico de Airbnb) al realizar pagos, retener fianzas etc, no realizan sin embargo el servicio subyacente al no ejercer un control o influencia significativa sobre el prestador del servicio (entre otras razones porque no fijan las condiciones ni el precio en el que se oferta la vivienda por parte del oferente del alojamiento).

Este y otros aspectos fundamentales deben ser objeto de revisión a la luz de la actuación de nuevos tipos de prestadores que no existían en el momento de la aprobación de la norma comunitaria pero cuya importancia por el volumen de negocio que generan y el número de actores implicados exige una solución normativa ad hoc. La la posición mantenida por el Tribunal de Justicia de la Unión Europea en su sentencia de 19 de diciembre de 2019, no parece que pueda despejar todas las dudas que planta la naturaleza

jurídica de estos prestadores y, por tanto, las consecuencias derivadas de su actuación frente a los particulares.

3. Los smarts contracts y su problemática.

La primera cuestión qué debe atenderse es cuál es la virtualidad práctica que tienen. Y acto seguido, si resultan útiles y si su utilización plantea problemas de orden jurídico. Realmente su virtualidad está ligada a la cadena de bloques. Los smarts contracts que se ejecutan en una cadena de bloques permiten solucionar algunos de los inconvenientes apuntados respecto de los contratos electrónicos, como son la manipulación el mensaje o la prueba de su emisión y recepción. Además, pueden utilizar el sellado de tiempo propio de las cadenas de bloques y su carácter inmutable. Cuestión distinta es que puedan considerarse contratos en el sentido técnico del término.

El resultado del smart contract tiene que ser la realización de algún tipo de prestación que pueda tener lugar en un entorno informático, siguiendo unas instrucciones que previamente se han dado al programa informático. Por ello, no parece posible que pueda generar prestaciones de trabajo. Otra cosa distinta es la relativa a las transacciones comerciales que tengan por objeto activos que sean susceptibles de representación e integración en el programa informático. Hablamos entonces de la tokenización de los activos. Un token es una representación digital de un activo real. Se obtiene utilizando un algoritmo matemático que a través de una función hast o función resumen, convierte el activo en un conjunto de datos representados en un código alfanumérico. Cada activo genera un hash único en la cadena de bloques.

cEstos activos pueden ser de diferente tipo. Pero entre ellos, sin duda, los instrumentos financieros son los idóneos para ser objeto de transacción a través de un Smart contrat. Del mismo modo que activos inmateriales de contenido patrimonial se han representado históricamente a través de títulos valores, cualquier activo de contenido patrimonial o económico puede ser representado mediante una huella digital, un token, dentro de la cadena de bloques. Tal y como ya sucede, por ejemplo, con las anotaciones

en cuenta en los mercados de valores, en la que la transmisión se realiza mediante apuntes en diferentes registros informáticos, los token son activos que tiene una representación contable y que pueden ser transmitidos mediante transferencias contables. Del mismo modo que en la anotación en cuenta, el titular será quien aparezca inscrito en el registro correspondiente.

En diferente plano se encuentran los bienes físicos, muebles o inmuebles. Es posible también tokenizarlos representándolos a través de un token. La cuestión es que la transmisión de ese token y el apunte en un registro contable no determinan en nuestra actual sistema inmobiliario que se produzca una modificación de la posesión del bien. En cuanto a los bienes corporales —un automóvil, un inmueble— el contrato inteligente puede automatizar un cambio de titularidad formal, de titularidad en un registro, mediante la tokenización del correspondiente activo, pero no un cambio en la situación posesoria. Entrarían en juego aspectos de gran calado en un nuestro sistema jurídico basado en la inscripción registral y la fe pública.

Como ya se ha señalado, se trata de un programa informático que se autoejecuta. La cuestión es qué consiste esa programación y si las partes afectadas cuando se ejecute están de acuerdo en los términos pactados. Y, por otra parte, hay otra cuestión esencial, y es la relativa a cómo obtiene el programa la información externa que necesita para ejecutarse en determinados supuestos y que no puede ser programada ab initio.

En relación con el primer aspecto, sería preciso que pudiera reunir los elementos que el Ordenamiento Jurídico requiere para su validez, tal y como han puesto de manifiesto por la doctrina que se ha ocupado del tema (MARTINEZ LABURTA, C. La revolución digital", AA.VV., Revolución digital, Dercho Mercantil y Token Economía 2019, págs. 437 y ss)., esto es, el consentimiento de las partes, un objeto cierto y una causa lícito, al margen de otros que deban concurrir. Se trata en definitiva de aplicar los criterios que en su momento se utilizaron para determinar la validez de los contratos realizados mediante un click.

En la contratación a distancia tradicional, la prestación del consentimiento se hace a través de los clásicos medios para la emisión de la voluntad, la forma escrita tradicional o la verbal. El problema que se plantea respecto a la prestación del consentimiento en la contratación electrónica es que la voluntad de contratar no se manifiesta en estos contratos de forma oral, ni siquiera en muchos supuestos de forma escrita, sino a través de gestos como puede ser clickear en el icono o botón que correspondan a aceptar (Web-wrap o Click-throug Agreements) . Las cláusulas escritas vienen sustituidas frecuentemente por conductas o actos de los contratantes, que evidentemente integran su voluntad negocial.

En la actualidad está resuelta la cuestión de si ante la ausencia de lenguaje convencional nos encontramos o no ante un auténtico consentimiento. El consentimiento contractual expreso no debe consistir de forma necesaria en una declaración escrita por parte del cliente en el terminal de su ordenador. Este podrá ser el caso de una aceptación escrita a través de un correo electrónico, pero la regla general en la contratación a través de la malla mundial es que la declaración de voluntad se manifieste ejecutando la orden "aceptar" , que resulta en sí misma eficaz . Nos encontramos ante un auténtico consentimiento, como además parece corroborar el hecho de que en la propia Ley de servicios de la sociedad de la información y de comercio electrónico se aluda de forma expresa al consentimiento en origen y en destino por medio de equipos electrónicos, de forma similar a lo establecido por la normativa comunitaria, sin establecer ulteriores precisiones.

En el ámbito de la contratación a través de Internet, donde podría circunscribirse también los acuerdos inter partes para establecer un Smart contrat, es preciso sustituir el concepto de declaración de voluntad, circunscrito a un momento y acto aislado, por uno más amplio de conducta negocial que pueda integrar en la voluntad de las partes no sólo las declaraciones expresas, sino también los hechos, gestos, silencios presunciones, lo que permite conectar con el concepto más amplio de "responsabilidad negocial" del artículo 1258 del Código Civil.

Respecto a la segunda cuestión que se apuntaba, la cuestión está en determinar cómo sabemos que el programa informático obtiene la información "exterior" correcta y

fiable y necesaria para poner en marcha la ejecución del contrato. El grado además de complejidad de la información puede variar ostensiblemente. No es lo mismo una información que puede ser contrastada a través de una fuente " oficial" (por ejemplo, horarios publicados por compañías aéreas, precios de valores cotizados, etc) que otra información que pueda tener algún componente subjetivo relativo a la idoneidad de la prestación. Esto nos lleva a los denominados "oráculos", que deben introducir esa información y que hacen que pueda plantearse dudas acerca de la fiabilidad del oráculo y su modo de influir en el smart contrat.

IV. PROPIEDAD INTELECTUAL EN ENTORNOS DIGITALES

1. Consideraciones generales

El entorno digital da lugar a la aparición de nuevos problemas relacionados con la propiedad intelectual motivados por el uso de tecnologías que no existían en el momento de publicación de los textos legales vigentes y a los que, por tanto, el Ordenamiento jurídico se debe enfrentar.

En general todos los sectores de la propiedad intelectual se ven afectados por la digitalización. En el contexto de los negocios *on line*, el nombre de dominio es en la práctica una de las formas básicas de identificación de un empresario e incluso de sus productos, aun cuando realmente su función es identificar y permitir el acceso a una página web. Esto choca con el Derecho de Marcas en el que se atribuye, como es sabido, la función de identificación de los productos y servicios de un empresario para diferenciarlos del de otro, a las marcas. También puede aludirse a los conflictos que surgen con los buscadores o comparadores de información, tan extendidos en la actualidad, que pueden en ocasiones conducir a resultados contrarios al Derecho de la Competencia. En relación con las patentes surgen interrogantes acerca de la patentabilidad de algunas invenciones relacionadas con las TICs a la vista de la exclusión de los programas de ordenador como tales programas.

Finalmente, los derechos de autor es uno de los ámbitos donde más se deja sentir la influencia de las TICs y por tanto, en el que el Derecho debe adaptarse para regular la coexistencia de estos derechos con el entorno digital dominado, cada vez más, por la tecnología de Big Data y por el almacenamiento de datos en la nube (cloud). Aspectos como la identidad digital, el derecho al olvido, y las nuevas formas de delincuencia asociados al entorno digital son aspectos igualmente que deben ser objeto de especial atención por el legislador.

2. Derecho de patentes.

2.1.La patentabilidad de la inteligencia artificial

Como es conocido, las patentes constituyen un factor determinante en el desarrollo de las economías industrializadas. La IA permite el desarrollo de una nueva generación de productos y servicios, incluso en sectores en los que las empresas europeas ya tienen posiciones sólidas: economía verde y circular, maquinaria, agricultura, salud, moda, turismo. La IA se usa para agilizar y optimizar las rutas de venta, mejorar el mantenimiento de las máquinas, aumentar la producción y la calidad, mejorar el servicio al cliente y ahorrar energía.

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. Nuestro entorno es cada vez más digital. La Inteligencia Artificial, la Automatización, la Realidad Virtual y la robótica están dando lugar a transformaciones tan relevantes en todos los sectores de suerte que ya comienza a hablarse de la cuarta revolución industria (4IR), caracterizada precisamente porque da lugar a nuevos sistemas que se construyen a partir de innovaciones que están protegidas, como es natural, por patentes.

Este tipo de invenciones se producen básicamente en los últimos diez años y el ritmo de crecimiento aumenta exponencialmente en los últimos. Básicamente, y 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, inteligencia artificial, 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. 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 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 OEP ha ido aclarando el art. 52, 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 (Oficina europea de patentes) 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.

2.2.Otras cuestiones problemáticas

La inteligencia artificial, como ya se ha señalado, cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo etc.). Pero al mismo tiempo, tal y como se pone de manifiesto en el Libro Blanco sobre Inteligencia artificial- un enfoque europeo orientado a la excelencia y la confianza, (COM/2020/65 final/2) la inteligencia artificial (IA) conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos.

Como ya se ha indicado, la inteligencia artificial y el internet de las cosas, en definitiva, una suma de algoritmos que han sido programados, pueden determinar el resultado de una relación contractual, sea del tipo que sea o incluso laboral. Piénsese, por ejemplo, en una elección de un candidato a un puesto de trabajo, o un proveedor basada en IA. El resultado al que se llega con los algoritmos no se motivan o explican. Solo quien programa el algoritmo y quien suministra la información de la que se nutre el programa, puede desgranar las razones que han llevado a proponer a un determinado candidato. Para ello debe conocerse las variables que se han tenido en cuenta, cómo ponderan cada una

de ellas, y los datos que a partir del modelo sobre el que se construye el algoritmo se suministran al algoritmo (DE LA QUADRA, pág. 47).

No se trata, desde luego, de un problema menor, pero sí de un problema no resuelto. Frente a la posibilidad de conocer la motivación de una decisión basada en IA, encontramos los derechos de propiedad intelectual del autor de los algoritmos – sin precisar, si se trata de una patente, o un derecho de autor- o de un secreto empresarial. Por otra parte, no parece que todas las situaciones puedan ser tratadas del mismo modo. Esto es, no es lo mismo situaciones en las que pueden verse afectados los derechos de las personas que otros supuestos. En el caso señalado, se podría vulnerar la tutela judicial efectiva si una decisión en una convocatoria pública no fuera debidamente motivada, puesto que esto generaría indefensión de cara a una posible reclamación; máxime teniendo en cuenta que los algoritmos pueden tener sesgos que podrían conducir eventualmente a resultados erróneos.

Puede mencionarse al respecto el Procedimiento Ordinario 18/2019 ante el Juzgado Central n.º 8 de lo Contencioso Administrativo, interpuesto por la Fundación CIVIO frente a la Administración, al negarse esta a facilitar el código fuente de una aplicación que realizaba una baremación que concluía con una adjudicación. La Administración utilizó como argumento la excepción existente en el artículo 14.1.j) de la Ley de Transparencia, límites al derecho de acceso, consistente en que se podrá limitar el derecho cuando "acceder a la información suponga un perjuicio para: […] la propiedad intelectual". y en la que lo que se dilucida es la posibilidad de conocer el código fuente. CIVIO, por el contrario, considera que, "*Mediante la imposibilidad de acceso al código fuente de los programas, el Derecho va derivando en una aplicación automatizada mediante un código binario imposible de leer, alejándose de esta manera ya no solo el principio de legalidad, sino todo tipo de posibilidades hermenéuticas, argumentativas y éticas*" (DE LA CUEVA, ¿Quién vigila al algoritmo? el Notario, 93 2020). Hay que señalar que el Tribunal Constitucional en su sentencia 55/2019, de 6 de mayo de 2019, en la resolución de un recurso de amparo interpuesto por una letrada contra la inadmisión de un escrito. En el Fundamento cuarto, apartado d) in fine, la sentencia del TC atribuye

a los ingenieros informáticos el establecimiento de los requisitos para poder formular recurso de casación, al introducir entre los campos de obligatorio cumplimiento en el formulario la selección de un código específico dependiendo de la modalidad de casación.

Otra cuestión diferente, es cuando la IA está dirigida a personalizar la publicidad o a establecer preferencias de un determinado tipo de público. En estos casos, parece mucho más obvio que deben prevalecer los derechos de propiedad intelectual.

Otra de las cuestiones que comienza a suscitarse al albur del desarrollo de la IA, es si puede ser considerado inventor un programa de IA; o si la creación generada por IA puede ser susceptible de protección como derecho de autor del programa.

Se trata de una cuestión que ya ha recibido una respuesta por parte de la Oficina Europea de Patentes y por las Oficinas del Reino Unido y Estados Unidos. A modo de prueba, como se reconoció por los promotores dela idea, se solicitaron en la Oficina Europea de Patentes (EPO en sus siglas en inglés) y en las oficinas señaladas sendas patentes dos patentes por el Artificial Inventor Project , designando al robot DABUS como inventor. LA EPO utiliza diferentes argumentos para denegar las solicitudes. Considera que la obligación impuesta en la normativa de indicar nombre y apellidos no se limita a un mero requisito formal que puede enervarse poniendo un nombre al robot, sino que se trata de un atributo propio de las personas que las capacita para ejercitar tales derechos. Derechos que como tales no pueden ser ejercidos por un robot. Con ello, solventa la cuestión por el momento. Aunque recordemos que todo gira en torno al reconocimiento de una "personalidad " a los robots. Ya recocemos "personas jurídicas" diferentes de las físicas, como construcción que precisamente permite reconocer a una organización un conjunto de derechos y obligaciones. Tendremos que esperar a ver si esto se produce también en relación con una "personalidad del robot", en cuyo caso los argumentos de la EPO, de carácter formal, decaerían.

Finalmente, guarda relación con el "inventor" el aspecto relacionado con la responsabilidad civil derivada de daños causados por productos o servicios basados en Inteligencia artificial. Es el caso de un vehículo autónomo que usando tecnología basada

en IA cause un accidente que provoque daños, personales o materiales. Ese resultado puede deberse a diferentes factores, entre los que puede encontrarse defectos en el diseño de la tecnología o en el proceso de aprendizaje dela máquina. La responsabilidad vinculada a daños causados por productos defectuosos recae siguiendo la normativa comunitaria en el fabricante. Pero no parece que puede realizarse sin más una traslación del esquema a productos que funcionan mediante tecnología de IA; máxime cuando se produce una cadena. Al final, la cuestión clave es determinar quién es el responsable del daño causado por un servicio o aparato que funciona con un sistema de IA. En el caso apuntado, ¿quién debería cubrir los daños: el propietario, el fabricante del vehículo o el programador?. Esa es la cuestión. Esto debe ser objeto de cuidado análisis, y de hecho, así se está haciendo en el seno del Parlamento Europeo donde se ha constituido una comisión especial para analizar estos delicados temas.

3. El conflicto entre nombres de dominio y marcas

3.1.El significado de los nombres de dominio

El nombre de dominio es una clave que se traduce en una secuencia gráfica cuya función es identificar y permitir el acceso a una página web. Los nombres de dominio pueden ser de primer y segundo nivel. Los de primer nivel consisten en un sufijo que aparece al final de la secuencia, que se asigna para un conjunto de actividades, vgr. ".com", para instituciones comerciales, o para un determinado país, vgr. ".es" para España. El de segundo nivel es el nombre de dominio concreto. Se forma anteponiendo al sufijo de primer nivel la denominación elegida por el solicitante para identificarse.

En España, la asignación de los nombres de segundo nivel del primero ".es" corresponde a la entidad pública española "Red.es", conforme a lo previsto en la DA 6ª de la LSICE y a la OM ITC/1542/2005 de 19 de mayo, que aprueba el plan nacional de nombres de dominio de internet bajo el código de país correspondiente a España —".es"—. La asignación se realiza sin comprobación previa del derecho del solicitante al nombre, de forma automática si se encuentra libre, salvo.gob.es y.edu.es. Además es

posible obtener el mismo nombre de dominio de segundo nivel pidiendo su asignación a la entidad extranjera encargada del registro de los nombres de primer nivel genéricos, fundamentalmente de los códigos ".com", ".net", o ".info", por lo que se podrá conseguir sin consideración a las normas españolas, siempre que no coincida con otro previamente asignado.

Pues bien, cuando la página web se utiliza para ofertar productos y servicios, el nombre de dominio se convierte en su signo identificativo de estos o del empresario dentro del comercio electrónico, cumpliendo, por tanto, un papel similar al que realizan las denominaciones sociales y los signos distintivos de la empresa. Esta circunstancia explica los problemas de compatibilidad que se generan en el tráfico entre aquellos y estos últimos, que están acrecentados porque los órganos competentes para asignar los nombres de dominio son distintos de los que otorgan las denominaciones y los signos distintivos y porque, según se ha indicado, la atribución se hace sin considerar derechos anteriores distintos de los propios nombres de dominio. La Ley, sin embargo, no ofrece una solución aceptable. Es verdad que en los supuestos en los que exista riesgo de confusión en el mercado pueden ejercitarse las acciones por confusión previstas en la Ley de Competencia Desleal y las normas sobre violación de signos distintivos registrados. La jurisprudencia española viene siendo muy proclive a ordenar la cancelación y el cese en el uso de los nombres de dominio que infrinjan derechos de marca anteriores por constituir denominaciones idénticas o similares a aquellas y utilizarse en el mercado para identificar productos o servicios idénticos o similares a los que comprenden tales marcas.

Sin embargo, la eficacia de esta solución es muy relativa ya que ambos tipos de acciones limitan su ámbito de aplicación al territorio español y puede muy bien suceder que la página web esté situada en un servidor fuera de esos territorios y, asimismo, el domicilio del operador económico titular del nombre también puede estar fuera de ellos, en cuyo caso se plantea el problema de la determinación del derecho aplicable. Es de destacar, no obstante, que el ICANN (*Internet Corporation for Assigned Names and Numbers*), que es la entidad encargada de controlar la atribución de nombres de dominio en internet, ha establecido una reglamentación para la resolución de conflictos entre

marcas y nombres del dominio, la *Uniform Domain Dispute Resolution Policy* de 24 de octubre de 1999, que encomienda la administración de las disputas relativas a los nombres de primer nivel genéricos, fundamentalmente de los códigos ".com", ".net", o ".info" al Centro de Arbitraje y Mediación gestionado por la Organización mundial dela Propiedad Intelectual (OMPI). Asimismo en la OM ITC/1542/2005 de 19 de mayo se prevé un sistema de resolución extrajudicial de conflictos entre estos y un catálogo más amplio de signos, como nombres comerciales o de empresas.

3.2.Colisión entre marcas y nombres de dominio

En el entorno digital cada vez son más frecuentes los conflictos entre las marcas y los nombres de dominio. Los derechos de marca tienen un ámbito de protección territorial que choca con el uso de los nombres de dominio en Internet, esencialmente extraterritorial. La Ley de Marcas, por ello, ya contempla la prohibición de usar una marca como nombre de dominio.

Esta prohibición afecta, desde un punto de vista estricto, al uso de direcciones de Internet sin el consentimiento del titular o licenciatario de la marca, así como el uso de esas direcciones de internet en páginas web, documentación de la empresa, etc. Y esto entra en colisión con el funcionamiento del registro de nombres de dominio (tanto del primer nivel, los *generic top level Domains*, como los territoriales, como es el caso del nivel "com" o el nivel "es").

El nombre de dominio se ha convertido, de facto, en uno de los signos distintivos de una empresa en Internet; es más, en numerosas ocasiones los tribunales se han pronunciado en el sentido de que el nombre de dominio cumple en Internet la función de marca. La sencillez del registro del nombre de dominio, en el que se aplica el principio *first to file*, en virtud del cual se adjudica el nombre de dominio al primero que lo solicita, con independencia que ese solicitante sea o no el titular de un derecho de marca sobre un signo idéntico o semejante, sea o no titular de un derecho marcario sobre

una denominación idéntica o semejante, ha dado lugar a que se produzcan registros de mala fe por parte de quienes se quieren aprovechar de la reputación o fama de una marca ya existente, en un fenómeno que se conoce como ciberocupación (*cybersquatting).*

En similares términos podemos referirnos a otro supuesto habitual como es el uso en internet de marcas de terceros previa comercialización de palabras clave vinculadas a enlaces publicitarios en motores de búsqueda (es el caso típico de *Google AdWords*). El problema se produce cuando se usan esas marcas o nombres comerciales como palabras claves de productos o servicios, de suerte que cuando se introducen determinados términos en la búsqueda que resultan idénticos a las marcas, se proporcionan enlaces patrocinados a sitios en línea que pueden ser competidores del titular o licenciatario de la marca o incluso donde se pueden ofrecer productos que imitan de la marca.

Se trata, entre otros, de claros ejemplos de colisión entre nombres de dominio con el tradicional Derecho de Marcas, pero también en relación con el Derecho de la competencia, dado que las actuaciones anteriormente descritas pueden constituir actos de confusión y actos desleales de explotación de la reputación ajena. El conflicto entre ambos sistemas dista de estar resuelto satisfactoriamente y exige nuevas soluciones adaptadas al nuevo entorno digital.

4. Los derechos de autor en el Mercado Único Digital.

Otro ámbito donde se está notando especialmente el conflicto entre las concepciones tradicionales y las nuevas propias del entorno digital es el de los derechos de autor. La evolución de las tecnologías digitales ha transformado la manera en que se crean, producen, distribuyen y explotan las obras y otras prestaciones protegidas. La evolución vertiginosa de las tecnologías en los últimos años ha posibilitado la copia y reproducción de las creaciones intelectuales con bastante facilidad y distribución y comunicación a través de redes sociales y plataformas sin el consentimiento de la persona autora de las mismas, que por otra parte, deja de recibir la contraprestación económica que le corresponde. El papel de las plataformas que alojan contenidos es un foco

permanente de conflictos, puesto que invocan para eximir cualquier tipo de responsabilidad respecto de los contenidos que alojan, el principio de neutralidad tecnológica. Aparecen también nuevas licencias pensadas para el mundo digital, como las *Creative Commons*.

El legislador consciente de esa dicotomía, inició un proceso de reforma de la Directiva en materia de propiedad intelectual que ha cristalizado en Directiva (UE) 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. En ella se establecen normas para adaptar determinadas excepciones y limitaciones a los entornos digital y transfronterizo, así como medidas destinadas a facilitar determinadas prácticas de concesión de licencias en lo que respecta a la difusión de obras que están fuera del circuito comercial y la disponibilidad en línea de obras audiovisuales en plataformas de vídeo a la carta con miras a garantizar un mayor acceso a los contenidos. A fin de lograr un correcto funcionamiento del mercado de los derechos de autor, también se incluyen normas sobre los derechos de edición, sobre el uso de obras y otras prestaciones por parte de los proveedores de servicios en línea que almacenan y facilitan acceso a los contenidos cargados por los usuarios, y sobre la transparencia de los contratos de autores y artistas intérpretes o ejecutantes.

En esta línea, en nuestro Ordenamiento El BOE del 2 de marzo de 2019 publica la Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

Aspectos claves son el reconocimiento de un derecho conexo para los editores de prensa en el entorno digital, dirigido a que los editores puedan obtener una remuneración por el uso de sus contenidos en Internet. También, las obligaciones de las plataformas digitales que permiten el acceso a contenidos protegidos por derechos de autor y el

incremento de sus deberes de colaboración con las autoridades en los supuestos de que se vulneren derechos de autor. Hay cuestiones de calado como la posibilidad misma de que las plataformas sean obligadas a bloquear el acceso a la web de los infractores, que cancelen su nombre de dominio o incluso que suspendan sus servicios de pagos electrónicos o publicidad. Nuevamente, el Ordenamiento jurídico debe lograr el equilibrio entre intereses jurídicos contrapuestos.

V. LA INCIDENCIA DE LA INNOVACIÓN DIGITAL EN EL MERCADO FINANCIERO

1. Contexto

Con la digitalización podríamos estar a punto de asistir a una trascendental transformación del sistema financiero, puesto que supone un poderoso motor de cambio de los bancos, del propio dinero y de los mercados de valores, que da lugar a la aparición de nuevos tipos de empresas y también de productos y servicios financieros.

La descentralización consecuencia de tecnologías como Blockchains, permitenreducir de forma notable los costes derivados de la intermediación financiera; pero paralelamente resulta susceptible de generar riesgos para la competencia en el mercado, sea por concentración de poder o prácticas concertadas en ciertos nodos, así como problemas para la supervisión del cumplimiento de la normativa que resulta aplicable en cada uno de los ámbitos del sector financiero (bancario, del mercado de valores y asegurativo), dirigida a procurar el buen funcionamiento del mercado y la protección de los usuarios de servicios financieros que se tornan objetivos prioritarios para el legislador, tanto en el ámbito de la Unión Europea como en el nacional.

Es evidente pues el impacto del fenómeno *Fintech* en las condiciones de competencia del sector financiero y por ende de toda la economía. Tal y como se señala en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité delas regiones sobre una Estrategia de Finanzas

Digitales para la UE (Comisión Europea. Bruselas, 24-09-2020. COM (2020) 591 final.) : " *El futuro de las finanzas es digital: Los consumidores y las empresas acceden cada vez más por la vía digital a los servicios financieros, los participantes en el mercado innovadores están desplegando nuevas tecnologías y los modelos empresariales existentes están cambiando*". Esta situación se ha hecho si cabe más evidente a raíz de la pandemia de COVID-19. Así, se ha incrementado las compras on line y con ello los pagos en red, lo que también ha ocurrido con los pagos en los comercios; una parte muy importante de transacciones se ha realizado utilizando infraestructuras digitales, y los propios empleados del sector financiero realizan teletrabajo.

El Derecho se enfrenta pues al reto de regular fenómenos desconocidos hasta el momento.

2. La aparición de las denominadas empresas fintech/insurtech

2.2.Consideraciones generales

El desarrollo de las nuevas tecnologías aplicadas a los mercados financieros ha dado lugar a la aparición de gran número de empresas bajo la denominación genérica de *FinTech* – aunque también está extendida la denominación de *InsurTech*- cuando se trate de empresas en el ámbito de los seguros- No existe un concepto unívoco, si bien en la práctica viene a agrupar a las empresas que efectúan desarrollos tecnológicos innovadores para el diseño, la oferta y la prestación de productos y servicios financieros. Generalmente, se trata de empresas de nueva creación (*start-ups*), de dimensión reducida, pero con una base tecnológica muy importante.

Cierto es que también han entrado en el sector las grandes empresas de base tecnológica, las denominadas Big-*Tech*, entre las que se encuentran, sin duda, Google, Apple, Microsoft, Facebook, Amazon o Alibaba Estas multinacionales unen el prestigio de su marca a la ingente información que disponen de sus clientes. Además de sus productos y servicios tradicionales actúan como canalizadores de pagos; del mismo modo

que su presencia es cada vez más acusada en el sector de los seguros, asociándose con start-ups innovadoras. Así Google, está actuando en las industrias automotriz y doméstica; Apple, en las empresas de salud, automóviles y domótica.; Facebook y Amazon, aprovechan recopilando datos y utilizándolos básicamente en el sector automotriz; y Alibaba ocupa una posición líder en la venta *online* de seguros.

Estas empresas *FinTech* en unos casos realizan actividades que ya se venían realizando, si bien lo hacen a través de nuevos canales. Así ocurre, por ejemplo, en los supuestos de captación de capital por parte del público inversor mediante la suscripción de valores; la particularidad es que se realiza a través de plataformas de financiación participativas que funcionan exclusivamente de forma telemática (*equity corwdfunding*); y en otros casos, este tipo de empresas realizan actividades que hasta tiempos recientes eran desconocidas, como podría ser, por ejemplo, el asesoramiento automatizado en inversiones (*roboadvisors*).

2.3.. Régimen jurídico: problemas relacionados con el Derecho de la competencia y con la protección de los usuarios de servicios financieros.

La cuestión que se plantea de inmediato es cuál es el régimen aplicable a este tipo de empresas FinTech. En el sector financiero, las empresas obtienen la autorización y están sujetas a un régimen de supervisión atendiendo al tipo de actividades, productos o servicios que desarrollan, con independencia de si utilizan métodos tradicionales o innovadores para prestar estos servicios. Y ello con el objetivo de garantizar por un lado, la estabilidad e integridad de los mercados; y por otro, la protección de los consumidores e inversores.

Por estas razones, desde los sectores tradicionales se señala que, tratándose de actividades propias de sectores regulados, como la banca, los mercados de valores y los seguros, a estas empresas les resulta de aplicación toda la normativa de supervisión

mercantil y administrativa, puesto que, de otro modo, compiten en condiciones de desigualdad y por tanto provocan situaciones de competencia desleal. Desde el sector de las empresas *FinTech* se señala la necesidad de adoptar un marco jurídico propio y adaptado a estos nuevos modelos.

En este sentido, la Autoridad Bancaria Europea aboga por permitir a estas empresas contrastar o probar su modelo de negocio con carácter previo a la solicitud de autorización, sin que se les aplique o, se haga de forma muy laxa, el régimen ordinario de autorización administrativa. Se trata de la denominada "licencia *sandbox*", que consiste en conceder un período de prueba controlado por las respectivas autoridades supervisoras en el que se les permite contrastar su modelo de negocio, tras el cual estarían sometidas al régimen de autorización propio del sector concreto –banca, bolsa y seguros-. Esta es la idea que, por otra parte, se recoge en el Proyecto de Ley de Medidas para la Transformación Digital del sistema financiero de 28 de febrero de 2020-: *Desde la óptica de las autoridades públicas el cambio acelerado, impulsado por las nuevas tecnologías y por los modelos de negocio basados en las mismas, supone, en primer lugar, un reto de adaptación tecnológica, pero también otro más fundamental: la política financiera tiene que garantizar que la innovación aplicada al ámbito financiero es segura y beneficia al conjunto de la sociedad. Se trata de facilitar el acceso a financiación como motor de la economía, asegurando que la transformación digital no afecte en modo alguno al nivel de protección al consumidor de servicios financieros, a la estabilidad financiera y a la integridad en los mercados, ni permita la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo.*

También debe tenerse en cuenta el "Plan de Acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador" elaborado por la Comisión Europea y publicado el 8 de marzo de 2018, en el que se recoge que los marcos reglamentario y de supervisión de Europa deberían permitir a las empresas que operan en el mercado único de la UE sacar partido a la innovación financiera y ofrecer a sus clientes los productos más apropiados y accesibles. Estos marcos deberían garantizar un alto nivel de protección para los consumidores e inversores, así como la resiliencia y

la integridad del sistema financiero. También deberían establecer medidas concretas para enfrentarse a los retos de estos nuevos modelos tales como el riesgo cibernético, las cuestiones relacionadas con la protección de datos, protección de inversores y problemas de integridad de los mercados.

Respecto a la existencia de mecanismos suficientes para proteger a los usuarios de estos nuevos productos y servicios financieros la entrada en vigor de la Directiva 2014/65/UE, de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros (conocida como la MiFID II) y del Reglamento (UE) 600/2014 de 15 de mayo de 2014 relativo a los mercados de instrumentos financieros viene a paliar algunas de las deficiencias que presenta el actual modelo. En nuestro país solo se ha implantado parcialmente mediante la modificación del TRLMV por Real Decreto-ley 14/2018, de 28 de septiembre. En todo caso, se trata de una regulación general que requerirá de desarrollos normativos adecuados y más específicos.

En relación con la protección de datos de los clientes y usuarios de los servicios financieros, la a UE consciente de estos importantes cambios, a través de su Estrategia para el Mercado Único Digital, propuesta por la Comisión Europea en 2015, empezó a sentar las bases para la creación de Mercado Único Digital libre y seguro en el que los ciudadanos puedan comprar en línea a través de las fronteras y las empresas puedan vender en línea en toda la UE. El objetivo de esa estrategia es lograr que la economía, la industria y la sociedad europeas aprovechen plenamente la nueva era digital. Junto a las innumerables ventajas que supone para las empresas poder disponer de esa ingente información que proporciona la tecnología referida, también aparecen riesgos importantes a los que el Derecho debe dar solución y que vienen referidos básicamente a otorgar la debida protección a los titulares de los datos personales que se obtienen y tratan.

En un contexto digital, los inversores inexpertos tienen acceso a un abanico cada vez más amplio de servicios financieros, incluidos unos servicios más baratos e innovadores. Las identidades digitales interoperables facilitarán el acceso a estos productos a distancia y a través de las fronteras. Paralelamente, al adquirir las empresas tecnológicas una mayor cuota del mercado de servicios financieros, estos inversores se

enfrentarán a riesgos adicionales a los que se contemplaban hasta el momento, además de una posible reducción de la competencia que finalmente restaría las ventajas.

En esta línea, como ya se ha indicado, la Unión Europea ha acometido un profundo proceso de revisión de la normativa existente creando un nuevo marco europeo de protección de datos, especialmente dirigido a las empresas que usan tecnología Big data, *y cuyas normal principales son el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (RGPD) y la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

Además, en la Estrategia de Finanzas Digitales para la UE, la Comisión fija un claro objetivo estratégico: adoptar las finanzas digitales en beneficio de los consumidores y las empresas. Y para ello, marca cuatro prioridades:

- La primera prioridad es poner fin a la fragmentación del mercado único digital de los servicios financieros, con el fin de permitir a los consumidores europeos acceder a servicios transfronterizos y de ayudar a las empresas financieras europeas a expandir sus operaciones digitales

- La segunda prioridad es garantizar que el marco regulador de la UE facilite la innovación digital en interés de los consumidores y de la eficiencia del mercado.

- La tercera prioridad es crear un espacio europeo de datos financieros para promover la innovación basada en los datos, a partir de la Estrategia Europea de Datos, mejorando también el acceso a los datos y su intercambio en el sector financiero.

- La cuarta prioridad es abordar los nuevos retos y riesgos asociados a la transformación digital.

Es importante abordar todos estos riesgos, no solo los que afectan a los clientes (tomadores de pólizas, inversores y depositantes), sino también los problemas más amplios de estabilidad financiera y competencia en los mercados.

Por ello, l Comisión, en su Estrategia ha adoptado un paquete de medias, con estrategias de Finanzas Digitales y de Pagos Minoristas, y con propuestas legislativas sobre criptoactivos y resiliencia digital.

3.La aparición de nuevos productos y servicios financieros

3.1. Nuevos sistemas y servicios de pago.

La tecnología aplicada a los servicios de pago es algo ya conocido en el ámbito financiero. Baste pensar en los sistemas de tarjetas y dinero electrónico, la banca móvil. Los avances en este ámbito han dado lugar no sólo a un modo de agilizar y abaratar los pagos, sino que ha sido un banco de pruebas en la generación de nuevos productos y servicios.

Entre los sistemas y servicios de pago encontramos nuevos agentes que compiten con las entidades financieras tradicionales y que permiten incrementar la competencia y movilizar servicios más personalizados o complementarios. La primera gran innovación es el monedero digital (*Digital Wallet, DW*), que puede funcionar como monedero *on line* (Online Wallet, *OW*) o como monedero móvil (*Mobile Wallet,* MW). Consiste en una herramienta de hardware y software que permite el almacenamiento de todos los datos necesarios para realizar el pago. Estos últimos están aportando nuevas funcionalidades puesto que permiten las transferencias de empresas a consumidores (b2c) pero también entre empresas (p2p) y de consumidor a consumidor (c2c).

En este proceso de innovación, vemos como va cambiando también el objeto del negocio tradicional. La banca ha utilizado lo sdatos de los clientes, pero estos nunca han sido el objeto de su negocio, que era el dinero, y los títulos. Los datos de los clientes ha sido una herramienta que además debían custodiar. Frente a esta postura, las empresas tecnológicas, tanto las denominadas GAFA como las empresas chinas denominadas BAXT (Baidu, alibaba, Xiaomi y Tecent) tienen como objeto de negocio los datos de los clientes.

Con ello se han convertido en competidores directos de la banca. Es probable que las empresas tecnológicas pasen a convertirse en actores habituales del ecosistema financiero.Esto ha hecho reaccionar a los bancos, que comienzan a utilizar también los datos como medio de expansión de su negocio tradicional.

Nos encontramos en ese sentido, en un proceso que ha facilitado la irrupción de nuevos proveedores de servicios de pago entre consumidores (*Third Party Providers* o TPPs), que siempre que cuenten con el consentimiento de estos podrán realizar "Servicios de iniciación de pagos" (*Payment Initiation Services* o PIS) a los proveedores del consumidor, y también realizar "Servicios de información sobe cuentas, (*Account Information Services*, AIS), accediendo a toda la información del titular de la cuenta y actuando sin necesidad de contraseñas para mejorar el conocimiento de la situación financiera del consumidor y de sus necesidades. Con este sistema en general los usuarios pueden controlar sus gastos de forma más directa y las empresas también podrán conocer mejor las transacciones que realizan los usuarios con los que trabajan, lo que les permitirá mejorar tanto su gestión interna (*back-office*), como su relación con terceros (*front-office*), a través de una oferta especializada y más personalizada.

La industria Fintech ha venido desarrollándose en n ámbito carente de regulación. Con el avance de esta operatoria los propios operadores han ido reclamando espacios seguros y las autoridades han comenzado a analizar los riesgos de estas operaciones y la necesidad de crear un mercado integrado de pagos. El Parlamento y la Comisión europea mantienen el principio de neutralidad tecnológica. Los servicios de pagos digitales se basan en la confianza de los usuarios, por lo que resulta esencial la protección de los

mismos. Para ello, se requiere una importante coordinación. Como se ha señalado, una regulación funcional exige una supervisión funcional (Competition issues in the área of Financial Tchology (Fintech) (July 2018) (pag. 15)- Disponible en : https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027_EN.pdf). La mayor complejidad técnica incrementa los riesgos que afectan a la seguridad de los pagos. A esto se une, que los procesos basados en inteligencia artificial pueden crear algoritmos difíciles de controlar (ZUNZUNEGUI, F., PÁG. 202. La digitalización de los servicos de pago,Fintech, REgtech y Legaltech: Fundamentos y desafíos regulatorios, Tirant lo blanch, 2020.La autoridad bancaria europea ha publicado informes a este respecto (https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/79d2cbc6-ce28-482a-9291-34cfba8e0c02/EBA%20FinTech%20Roadmap.pdf

Aunque la Segunda Directiva sobre Sericios de Pago supuso un importante avance en la protección de los ususarios de servicios de pago, es un texto que necesita revisión para ser adaptado a este nuevo entorno digital.

3.2.El dinero digital: las cripto-monedas

Junto con estos nuevos instrumentos de pago, que parten de la existencia de dinero físico que circula por medios electrónicos, y al que puede denominarse dinero electrónico, y que ha sido objeto de regulación por el legislador comunitario, debe mencionarse como gran innovación el dinero digital, que parte de la tecnología *Blockchain* y que no tiene la consideración de moneda de curso legal. El Banco Central Europeo considera que se trata de la representación digital de valor, que pueden ser intercambiadas por medios telemáticos y que sirven como instrumentos de cambio y unidad de valor o de almacenamiento de un valor, si bien esas funciones las cumple por el acuerdo de la comunidad de usuarios que utilizan el sistema. Dentro de estas criptomonedas el ejemplo típico son los *bitcoin*, que siguiendo lo indicado, es una moneda digital que parte de la

tecnología *Blockchain* y cuyo valor de cambio viene dado por la aceptación de los que se asocian al sistema contable *bitcoin.*

Es obvio que este sistema descentralizado puede reportar ventajas, pero también que siguen siendo muy importantes los problemas jurídicos pendientes de resolver como el acceso a datos de cuentas bancarias, aspectos de protección de los usuarios de los servicios, posibles problemas de competencia, incluso posibles riesgos sistémicos si se detectaran fallos en la tecnología.

En efecto, uno de los aspectos problemáticos es el relativo a la privacidad de los datos personales. SE trata de un aspecto especialmente importante en las criptomonedas basadas en blockchain públicas, que son precisamente en las cuales se basan algunas de las criptomonedas más extendidas. Si algún nodo revelara qué persona está detrás de la clave pública, se podría llegar a conocer todas las transacciones realizadas. Los problemas de competencia pueden surgir por el hecho de que pocas empresas almacenen y traten un volumen significativo de datos, así como por el hecho de que resulta notorio ya que se crean acuerdos entre los mineros que actúan como parte esencial en el funcionamiento de la cadena de bloques, y que pueden llegar a acuerdos entre ellos, de modo que si se alcanza el 50% de la minería, se puede controlar la cadena de bloques (EYAL, I/ GÄUN, E., MAYORITY IS NOT ENOUGH: Bitcoin mini gis vulnerable. Communication of the ACM 95-102 (2008). Disponible en https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf). A esto se suman los problemas relacionados con la ciberseguridad.

Aspectos que, entre otros, están siendo tenidos en cuenta en la revisión de la D*irectiva (UE)* 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior en lo que ya se conoce como Segunda Directiva de Servicios de Pago (*Revised Directive on Payment Services 2*, PSD2). Uno de los principales aspectos a tener en cuenta y que puede suponer un cambio trascendental para el sector bancario es la consagración de la figura de los proveedores de servicios de pago a terceros o TPPs (*Third Party Payment Service Providers*) al otorgarles acceso a la

infraestructura de los bancos bajo la supervisión, igual que los bancos, de la Autoridad Bancaria Europea (ABE).

Además, consciente de la problemática que plantea este instrumento, pero también de sus ventajas, la etrata del «Reglamento sobre los mercados de criptoactivos» (Proposal for a REgulation of the European Parliament and the Council on Markests in Crypto-assets, and amendin Directive (EU) 2019/1937. Bruselas 24.09.2020. COM (2020) 593 FINAL). Se trata de un documento que requiere de un análisis minucioso, puesto que es fundamental a la hora de aportar claridad y seguridad jurídicas a los emisores y proveedores de criptoactivos. Las nuevas normas permitirán a los operadores autorizados en un Estado miembro prestar sus servicios en toda la UE («régimen de pasaporte»). Las salvaguardias incluyen requisitos de capital, custodia de activos, un procedimiento obligatorio de reclamación a disposición de los inversores y derechos del inversor frente al emisor. Además, deben analizarse cuáles son los requisitos que se van a exigir en términos de capital, supervisión y derechos de los inversores a los emisores de las denominadas criptomonedas estables», es decir, aquellas respaldados por activos significativos a nivel mundial.

También resulta muy importante y debe seguirse con especial atención el "entorno de pruebas" (sandbox) que propone la Comisión para las infraestructuras de mercado, pensado para que tanto los reguladores como pas empresas puedan adquiriri experiencia en el uso de la tecnología Blockchain, rebajando o excepcionando requisitos aplicables con carácter general.

3.3.Neobanks y challenger banks

La banca está asistiendo a una profunda transformación. Hay un importante cambio tecnológico, que va acompañado por un cambio cultural. Los ciudadanos tienen nuevos hábitos derivados de una mayor educación digital. Las transacciones ordinarias se hacen ya de forma habitual sin la presencia física en las entidades bancarias. También

factores coyunturales económicos influyen en este cambio de paradigma en la actuación de las entidades bancarias y su relación con sus clientes.

Tradicionalmente, la banca venía obteniendo un amplio margen de beneficio con lo que eran sus actividades principales: la concesión de préstamos y las operaciones con productos financieros de renta variable. En relación con el primer aspecto, las circunstancias han cambiado notablemente. La bajada de los tipos de interés ha supuesto una bajada importante de la rentabilidad de la banca. Los tipos de interés de los préstamos siguen bajando, y os depósitos a cuenta ya no tienen ningún tipo de interés ni para los clientes ni para las entidades, que a diferencia de lo que era natural, tienen que pagar comisiones en lugar de recibir intereses. Esto influye lógicamente en la huida de los clientes de este tipo de productos, y como contraparte, que las entidades bancarias también busquen otro tipo de actividades y productos que impliquen un valor añadido para los clientes. Respecto a la venta de productos financieros, cabe recordar que los controles impuestos por la normativa comunitaria se han intensificado al objeto de paliar las actuaciones de las entidades en sus relaciones con sus clientes más inexpertos. Ha habido importantes escándalos financieros que también han minado la confianza de los clientes en el sector.

Conocer este contexto es necesario para comprender cómo está evolucionando el sector. En un mercado cada vez más digital, la experiencia del usuario será la principal ventaja competitiva y determinará el crecimiento y supervivencia de las empresas (DIÉZ GARCÍA, D./GÓMEZ LARDIES, G., " El impacto de la blockchain en las diferentes industrias. Banca y Blockchain, ¿pioneros por necesidad?, Blockchain: La revolulción industrial de Internet, (Coor. A. Preukschat). GEstion 2000, Barcelona, pág. 36). En este sentido, además de las denominadas empresas GAFA,(Google, Apple, Facebook y amazon), han aparecido empresas que frente a la dificultad de la banca de adaptarse a la nueva situación, han optado por innovar, creando nuevas figuras, dotadas de mayor flexibilidad, agiles y totalmente orientadas al cliente. Tal es así, que esta nueva línea de negocios se extiende hasta países en los que no se ha asentado la banca tradicional.

Por tanto, nos encontramos en un momento en el que las empresas han centrado su foco en el cliente. Ya no se trata tanto de competir por lanzar el mismo producto en el mercado con mejores condiciones para el cliente, sino en centrarse en los nuevos hábitos de consumo y expectativas de los clientes.

En este contexto, deben situarse los denominados "neobancos" (neobanks) y especialmente los *challenger banks*, cuya característica común es que se trata de plataformas de nueva creación que ofrecen un abanico integral de productos bancarios en competencia directa con los bancos clásicos. Los denominados challenger *banks*, son entidades de crédito con funciones similares a las tradicionales, pero con un funcionamiento completamente digital. Los neobancos, por su parte, ofrecen, junto a las funciones básicas de los bancos, otras funciones, pudiéndose centrar únicamente en la realización de actividades complementarias o aspectos concretos del sector. Y ello lo hacen asociándose con las entidades de crédito que no tienen un funcionamiento digital, generalmente mediante aplicaciones móviles. Aunque hasta el momento vienen desarrollando servicios similares a los de esa banca tradicional, se espera que sean las impulsoras de la operativa con cripto-monedas.

La tecnología de registro distribuido descentralizado resulta una gran aliada en este nuevo escenario. Los pagos globales en la actualidad se realizan a través de diferentes proveedores de pagos, siendo el más conocido, SWIFT. A través de este sistema, los bancos pueden conectarse y determinar la existencia de una transferencia internacional, dotando de seguridad tanto al emisor como al receptor de la misma (GÓMEZ LARDIES, G./DÍEZ GARCÍA, D., " Las aseguradoras se reinventan", Blochain: la revolución industrial de Internet (coor. A. Preukschat,Gestión 2000,2017, pág.. 38), Este sistema requiere para su realización un período de tiempo que oscila entre 2 y 5 días. Este tiempo puede reducirse de manera sustancial utilizando blockhain, que podrían ser públicas – el caso paradigmático es bitcoim y Ethereum- o privadas – el caso de Riplle-. Por otra parte, hasta cabe imaginar que la Blockchain sea una herramienta para facilitar la concesión de préstamos sin la necesidad de entidades financieras tradicionales.

3.4.Financiación participativa (crowdfunding). ICOs

La financiación participativa (*crowdfunding)* a grandes rasgos es un sistema que se basa en una llamada abierta al público para obtener financiación para un proyecto específico a través de internet. Supone por tanto una desintermediación en la financiación de los agentes, ya sea en forma de capital (E*quity crowdfunding, ECF*) o de préstamos (P2P *lending*). Estos tipos de financiación se regularon en la Ley 2/2015, de 27 de abril, dirigida a dar carta de naturaleza a estos sistemas a la para que estableciendo unas normas básicas de protección a los inversores. Este tipo de financiación supone una desintermediación respecto de los intermediarios financieros tradicionales como son las entidades financieras. En este tipo de financiación, una plataforma utilizando como elemento esencial la tecnología ofrece servicios propios de gestión y comercialización de servicios financieros, que permiten poner en contacto a muchos sujetos que aportan su inversión (*crowdfunders*). Es la tecnología la que facilita que cualquier proyecto empresarial pueda llegar a muchos inversores con independencia de su localización geográfica. Las oportunidades tanto para los emprendedores como para los potenciales inversores ha llevado a que su crecimiento en los últimos años resulte exponencial.

Las ventajas se ven acompañadas, no obstante, de riesgos para los inversores en algunas situaciones, que han intentado ser paliadas por la normativa existente, aunque el hecho de que sea un fenómeno global impide que el ámbito de protección de una normativa nacional pueda resultar satisfactorio. Uno delos problemas con los que se pueden encontrar los inversores es con la deficiente información que se proporciona, que incluso puede no ser la correcta. No hay una estandarización de la información a proporcionar, lo que hace que, en cada caso, se ofrezca la que se estime oportuna. Los riesgos relativos a la ciberseguridad están igualmente presentes, como en todos los casos en los que las transacciones se realizan a través de las redes.

En esta evolución sin precedentes, nos encontramos con un disruptivo sistema de financiación en masa, las llamadas *Initial Coin Offerings* (ICOs) por analogía con las ofertas públicas de venta de acciones (*Initial Public Offering*, IPO). No obstante, las ICOs presentan diferencias importantes, puesto que lo que adquieren los financiadores no es

una acción o participación, sino una criptomoneda, y en particular, un *cripto-token*. Todos los usuarios del sistema tienen acceso al registro de las titularidades de esos *token*, y su titularidad se acredita en un sistema de clave pública y privada basado en la criptografía. Desaparece por tanto la figura del intermediario (no solo de la banca, sino también de la plataforma).

Este sistema es el mismo en el que se basan un tipo de criptomoneda como el *bitcoin*. La diferencia estriba en que mientras que el *bitcoin* viene a ser el equivalente a una moneda- puesto que trata de servir como medio de pago o como forma de almacenar un valor, el *token* representa un derecho o un bien determinado. El siguiente paso es el de equiparar el *token* a un valor negociable (*security)*, hablando entonces de *security tokens*.

Este sistema que comienza a desarrollarse presenta junto a sus ventajas también importantes riesgos relacionados con la protección de los inversores. La cuestión de fondo es si deben ser objeto de regulación y supervisión por parte de las autoridades de los mercados de valores y en caso afirmativo, con qué especialidades. En nuestro país, la CNMV ha señalado en una nota informativa que las ICOs quedarán sometidas a la normativa del mercado de valores cuando los "*tokens" atribuyan derecho o expectativas de participación en la potencial revalorización o rentabilidad de negocios o proyectos .. u otorguen derechos equivalentes o parecidos a los propios de las acciones, obligaciones u otros instrumentos financieros incluidos en el artículo 2 TRLMV*". No obstante, no se ha registrado ninguna ICO y no existe ningún mecanismo de control, por lo que deberá plantearse a buen seguro que no basta con extender la legislación general sino que es preciso buscar soluciones jurídicas *ad hoc* que concilien los diferentes intereses en juego.

3.5.Asesoramiento y gestión de carteras.

En el asesoramiento y gestión de carteras, también se están produciendo cambios motivados por las innovaciones tecnológicas. desde los comparadores financieros, pasando por agregadores financieros, plataformas de *networking* y percepción

(sentiment) en los mercados financieros, social trading, plataformas de negociación electrónica y *roboadvisors*.

Entre sus ventajas, el hecho de que facilita el acceso a este tipo de productos a un público mucho más amplio que el tradicional, y además a unos precios más reducidos, al producirse una importante desintermediación. Estas ventajas han sido puestas en valor por nuevas empresas tecnológicas (MERCADANTE, K., Robo Advisors: 5 Advantages to Automates Investing (2006) Disponible en : https://cashmoneylife.com/investing-with-robo-advisors/), que han venido a llenar un vacío de la banca tradicional, y que han jugado también con la desconfianza existente por parte de los ciudadanos ante la posición de dominio de las grandes entidades bancarias.

En relación con los roboadvisors, se plantea la cuestión de si un programa informático, es decir un conjunto de algoritmos , puede conocer las preferencias de inversión de un cliente y además puede cumplir toda la normativa existente. La práctica está demostrando que estos programas que cuentan con un ingente volumen de información tanto de los mercados como de los clientes, pueden efectivamente facilitar servicios de asesoramiento y hacerlo a un coste mucho menor y respetando el marco normativo existente. La utilización de la inteligencia artificial unida al *Deep learning y machine learnig*, puede dar lugar a resultados muy eficientes al poder gestionar un número ilimitado de clientes en relación con un número muy elevado de productos financieros, cualquiera que sea la complejidad de estos.

No obstante, las ventajas señaladas, lo cierto es que existen muchos interrogantes sobre su régimen jurídico. Los problemas como en otros casos de innovaciones tecnológicas es la inexistencia de controles y de supervisión, y por tanto, de protección a inversores inexpertos, así como de asegurar la propia estabilidad del mercado financiero. Entre los aspectos que deberán ser contemplados se encuentra los requisitos de constitución jurídica de estos robo-advisors, bien integrados en una empresa de servicios de inversión, o como empresa de servicios de inversión. Será esencial determinar cuál es el régimen de responsabilidad en caso de fallos del sistema y cómo se pueden combatir los problemas de ciberseguridad. Asimismo, un aspecto transversal, es fundamental

determinar cómo va a realizarse el procesamiento de los datos y cómo se va a proteger la privacidad de los inversores. Por otra parte, tal y como es una constante en el ámbito financiero, se hace preciso determinar de qué modo se va a supervisar el cumplimiento normativo por parte de los robo-advisors.

3.6.InsurTech

También en el ámbito de los seguros, se están produciendo cambios importantes. Nos encontramos, de un lado, con un nuevo tipo de cliente, que igual que para otros ámbitos, cada vez exige más y quiere comparar los diferentes productos existentes en el mercado, los servicios que se ofertan y las condiciones que las compañías aseguradoras establecen en las pólizas.

Ello hace que la competencia en el sector crezca y que las compañías cada vez opten por ofrecer productos más adaptados a los perfiles de sus clientes. Las innovaciones tecnológicas están suponiendo la aparición de nuevos productos más especializados, que permiten que el consumidor se involucre más y tenga acceso más fácil a la información (*Insurtech*).

Tener información acerca del cliente ha resultado siempre fundamental para las compañías aseguradoras para medir el riesgo en los productos asegurativos que ofrecen. En la actualidad, la tecnología Big Data, permite el acceso y recopilación de múltiples datos – piénsese en temas relacionados con las multas que tenemos, nuestras preferencias para viajar, nuestro estado de salud, etc. Ante mayor y mejor información, las compañías aseguradora puede ofrecer soluciones mucho más personalizadas, y mejorar su gestión interna, lo que incide en un cálculo más ajustado del riesgo, y por ende, de la prima.

Pero además, la utilización de la blockhain con ssmart contract puede resultar también un punto de inflexión en el modelo de negocio del sector asegurador Este registro descentralizado tiene capacidad tanto para almacenar como para gestionar y transmitir volúmenes muy importantes de datos, y hacerlo de forma fiable, en el sentido de que

permite garantizar la integridad de los datos. Hay muchas eventualidades que pueden contemplarse expresamente y que pueden permitir que se adopten soluciones automáticas mediante la ejecución del Smart contract. Es fácil pensar en la anulación de un billete de cualquier tipo de transporte por una circunstancia que no depende de la voluntad del viajero, y que este viajero cuente con un seguro de reembolso para esas circunstancias. La contratación tradicional conlleva que el titular del seguro interponga una reclamación, el agente de seguros realice una validación, se realicen transacciones con una entidad financiera, y todo ello, haga que el cliente reciba su indemnización pasado un mes. En el caso de que se utilizara una blockhain, tanto en una cadena pública, como en una privada – que podría ser más factible a corto plazo- bastaría con que el viajero en la página web donde va a concertar el vuelo, cuando le aparece la pantalla de contratar seguro por retraso, concertara ese seguro, indicando sus datos, como se quiere recibir la devolución, pague mediante una pasarela de pagos y finalmente reciba la notificación de que ha contratado el seguro. Si llegado el día del viaje, se produce el retraso, la aplicación de la compañía aseguradora ejecutará el contrato inteligente utilizando los datos que previamente facilitó el viajero. La aplicación (contrato inteligente) utilizando la información disponible en las webs oficiales (aeropuerto, trenesm, etc), comprobará la existencia del retraso en los términos establecidos en el contrato, y de ser así, efectuará el pago en la cuenta indicada (si fuera en criptomonedas de forma casí inmediata). Esa información permanecería en la blockhain lo que permitiría comprobaciones o auditorías posteriores.

En este caso, si el viaje se anula, sin necesidad de ningún tipo de reclamación, se ejecutará el Smart contract y el viajero recibirá la indemnización que hubiera estipulado. O en el sector de la agricultura, la previsión de circunstancias que pueden hacer malograr las cosechas y que testadas por medios digitales, permitan el cobro por parte del agricultor. Uno de los ámbitos donde también se están haciendo pruebas de casos con contratos inteligentes es en el del automóvil, industria que como es sabido mueve mucho dinero, y en la que puede redundar en un beneficio tanto para los titulares de los seguros, que pueden optar por las pólizas que más se adapten a sus necesidades, como para las compañías que puede reducir las tramitaciones y ahorras costes (GÓMEZ LARDIES,

G./DÍEZ GARCÍA, D., " Las aseguradoras se reinventan", Blochain: cit. pág.44 y ss). Proponen el siguiente ejemplo. Supongamos que un conductr quiere hacer un seguro del automóvil y que gracias a un sistema de Blockchain puede transmitir, de forma anónima y confidencial, su historial de siniestros para que sea valorado por diferentes compañías. Además, si se tratara de un vehículo que estuviera sensorizado aplicando el Internet de las cosas, podría completarse el informe con los hábitos de conducción de la persona. Si el conductor transmite esa información, diferentes compañías aseguradoras podrían enviarle contratos que serian ejecutados mediante Smart contrats, con ofertas de las compañías. Todos los trámites podrían hacerse de forma digital).

Además, las compañías pueden utilizar esas innovaciones tecnológicas para combatir el fraude, puesto que pueden cruzar datos obtenidos de diversas fuentes que les pueden permitir comprobar si el siniestro ha sucedido realmente o el momento en el que ha sucedido. Por otra parte, el que cada contrato quede almacenado en la cadena de bloques (resulta indistinto para ello que sea permisionada o no), dificultará la posibilidad de alterar la información contenida en los mismos. Además, permite diseñar productos específicos para determinados perfiles de clientes.

Y, además, en un contexto en el que las TICs han dado lugar a objetos inteligentes (el internet de las cosas, IoT), se plantean nuevos tipos de seguros para cubrir las eventualidades que surjan de ese nuevo modo de funcionar – baste con pensar en los seguros de los coches autónomos-. Se abre, por tanto, un nuevo espectro de necesidades asegurativas derivadas de la incidencia de la digitalización de la actividad económica.

VI. INCIDENCIA DE LA DIGITALIZACIÓN EN EL FUNCIONAMIENTO DE LAS SOCIEDADES

Las TICs se han ido incorporando de forma progresiva en el ámbito societario; es el caso por ejemplo de la incorporación del Documento Único Electrónico (DUE) en la constitución de sociedades, la legalización y presentación telemática de las cuentas anuales, etc. No obstante, la innovación digital, y en particular, la tecnología Blockchain

puede contribuir a dar un salto cualitativo en la digitalización del Derecho de Sociedades. El funcionamiento de este sistema que no requiere un tercero de confianza, pero que ofrece toda la seguridad material de que los contenidos no se pueden modificar y pueden ser conocidos por todos, puede afectar a aspectos básicos del funcionamiento de las sociedades, tanto en la esfera interna como en la externa. En este sentido, resulta especialmente importante la incorporación a nuestro Ordenamiento de la Directiva europea 2019/1151 de 20 de junio de 2019, sobre utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades, que viene a modificar la Directiva codificada 2017/1132 sobre sociedades, que ha refundido en un solo texto todas las Directivas vigentes, excepto la relativa a las sociedades unipersonales. El objetivo de la Directiva, tal y como se señala en su Exposición de Motivos, es facilitar la constitución de sociedades y el registro de sucursales, y de reducir los costes, el tiempo y las cargas administrativas asociados a tales procesos, en particular para las microempresas y las pequeñas y medianas empresas (pymes)

En la esfera interna, la tecnología Blockchain puede contribuir a mejorar el funcionamiento de los órganos sociales, logrando que se puedan gestionar de forma más efectiva las relaciones internas. Así puede facilitar, con todas las garantías, el modo de acreditar la representación de los socios, o el modo de comunicación de la sociedad con sus socios; o la sustitución de las reuniones presenciales por telemáticas. En particular, respecto de las sociedades cotizadas, puede contribuir a solucionar los problemas existentes en los casos en los que hay una disociación de la titularidad formal y real de las acciones (empty voting). El objetivo es que la sociedad emisora pueda conocer quienes son los inversores últimos y por tanto a quien corresponde en realidad el voto, máxime en los casos de voto transfronterizo. La nueva tecnología permite la elaboración de la lista de socios legitimados para asistir a la junta general y, por tanto, otorga certidumbre acerca del titular real de las acciones de la sociedad y, por tanto, sobre la identidad de los socios y el número de acciones poseídas. También resulta de especial utilidad su aplicación para el cómputo de los votos, como de hecho se realiza ya en algunos estados de Norteamérica, como Delaware o en Arizona. De este modo se logra la trazabilidad del voto, lo que cierta-mente es muy complicado en los casos en los que

se hace a distancia y hay entre el titular real de la acción y quien efectivamente vota en la junta una cadena de intermediarios financieros.

En la esfera externa, una de las principales aplicaciones de la tecnología Blockchain tiene que ver con el régimen de transmisión de las acciones y participaciones sociales que se supedita, como es sabido, a la inscripción en los correspondientes libros de registro establecidos en la LSC.

Finalmente, con carácter general, la aplicación de la tecnología Blockchain puede facilitar la supervisión por parte de las autoridades de control. Ejemplos posibles son el control del cumplimiento de las operaciones de autocartera a tenor de lo dispuesto en el Reglamento 596/2014, del Parlamento Europeo y del Consejo, de 16 de abril de 2014 sobre el abuso de mercado, o la elaboración de listas de iniciados a que alude el art. 230 del Texto Refundido de la Ley del Mercado de Valores en relación con el abuso de información privilegiada.

INTELIGENCIA ARTIFICIAL. CONFIGURACIÓN JURÍDICA Y EXAMEN DE SU CARÁCTER TÉCNICO.

Esperanza Gallego Sánchez.
Catedrática de Derecho Mercantil.

Sumario. I.PRELIMINAR. 1. Contexto. 2. Delimitación. II. EL DERECHO DE PATENTE SOBRE LA INTELIGENCIA ARTIFICIAL. 1. Planteamiento. 2. El carácter técnico.3. LA COMPATIBILIDAD DEL SISTEMA DE PROTECCIÓN MEDIANTE PATENTE CON OTROS SISTEMAS DE PROTECCIÓN. EL DERECHO DE AUTOR Y LOS SECRETOS EMPRESARIALES. Bibliografía.

RESUMEN. La inteligencia artificial es una expresión ampliamente difundida en informes, conferencias y otros actos de carácter esencialmente divulgativo. Pero carece de unos contornos mínimamente seguros que es necesario acotar cuando se trata de analizar las formas jurídicas que pueden utilizarse para su protección. En este trabajo se aborda la caracterización relevante de la misma desde el punto de vista jurídico como paso previo para estudiar su patentabilidad. En este ámbito se analiza su carácter técnico considerando las Decisiones de la Sala de Recursos EPO y las Directrices EPO, que no mantienen criterios coincidentes en todos los casos. Se defiende asimismo la acumulabilidad de este sistema de protección con el que deriva del derecho de autor y de la legislación sobre secretos empresariales.

I. PRELIMINAR.

1. Contexto.

La inteligencia artificial (en adelante IA) se inscribe de lleno en la llamada cuarta revolución industrial, 4IR, o industria 4.0., fenómeno que, a grandes rasgos, hace referencia a la introducción de las tecnologías digitales en la industria concebida en sentido amplio. 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. La singularidad del proceso consiste en que esa

introducción consigue 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.

En este contexto, al dar sentido a grandes cantidades de datos para ofrecer soluciones eficientes, la IA mejora los productos, procesos y modelos de negocio en todos los sectores económicos. Puede, por ejemplo, ayudar a las empresas a identificar qué máquinas necesitan mantenimiento antes de averiarse. Pero, tal y como constata 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, y su Anexo los usos de la IA no se circunscriben a la industria. Utilizamos la IA a diario, por ejemplo, para bloquear el correo no deseado o hablar con asistentes digitales. Está a nuestro alcance, cuando traducimos textos en línea o usamos una aplicación móvil para encontrar la mejor manera de ir a nuestro próximo destino. En casa, un termostato inteligente puede reducir las facturas de energía hasta en un 25% al analizar los hábitos de las personas que viven en ella y ajustar la temperatura en consecuencia. En el sector sanitario, los algoritmos pueden ayudar a los dermatólogos a realizar un mejor diagnóstico, por ejemplo, detectando el 95% de los cánceres de piel aprendiendo de grandes conjuntos de imágenes médicas. La IA también transforma los servicios públicos.

El potencial que se advierte en ella ha motivado una atención creciente hacia la misma no solo por parte de los sectores económicos implicados, sino también por las instancias públicas. Son escasos los países y organizaciones internacionales que no han iniciado acciones para promoverla y regularla.

A pesar de ello y de que es un término ampliamente difundido en informes, conferencias y otros actos de carácter esencialmente divulgativo carece de unos contornos mínimamente seguros. No se trata de los sectores a los que afecta, o a los que podrá afectar, que, naturalmente, están en permanente evolución, y ahora no pueden, ni deben, ser determinados. Se trata de acotar un supuesto de hecho en atención a las características que lo definen, actuación imprescindible cuando se pretende ligar al mismo determinadas consecuencias jurídicas. Máxime cuando esas eventuales consecuencias jurídicas determinan la existencia de derechos de explotación exclusiva y afectan a los derechos de terceros.

2.Delimitación.

En atención a ello conviene contar con una formulación que, sin dejar de ser amplia, al objeto de permitir que comprenda ulteriores ámbitos exigidos por la innovación tecnológica, no resulte extremadamente ambigua o carente de contenido, tal que impida decidir el régimen jurídico de protección de la misma. Un óptimo punto de partida a este respecto es recurrir, en primer término, a los creadores de la expresión. Es común afirmar que el origen de la IA se encuentra 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 allí un programa de ordenador, el "*Logic Theorist*, que emulaba características propias del cerebro humano y que es considerado el primer sistema de inteligencia artificial puesto que era capaz de demostrar los teoremas sobre lógica matemática expuestos en los tres volúmenes de los "*Principia Mathematica"* de Alfred N. Whitehead y Bertrand Russell (1910-1913) (NAVAS NAVARRO, S. "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en AA. VV. *Inteligencia artificial,* Valencia, Tirant lo Blanch, 2017, págs.24 y 25). Sin embargo, parece que el término fue acuñado por John McCarthy, otro de los participantes, quien definió la AI 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. Se trata, en definitiva, de 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 (NAVAS NAVARRO, S. "Derecho e inteligencia artificial desde el diseño. Aproximaciones", cit., pág. 24).

En este mismo sentido la norma ISO/IEC 2382:2015(en), 212377, sobre Información tecnológica (https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en) define la IA como la capacidad de una unidad funcional para realizar funciones que generalmente están asociadas con la inteligencia humana, como el razonamiento y el aprendizaje. Y 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-Inteligencia artificial para Europa de 25 de abril de 2018 (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES) determina que el término se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos.

En definitiva, se trata de un concepto que remite al esfuerzo por reproducir digitalmente estructuras de decisión similares a las humanas, es decir, a concebir un ordenador, y, sobre todo, a programarlo de modo que pueda procesar problemas con la máxima autonomía posible y, en su caso, desarrollar los programas empleados. El objetivo es solventar tareas especialmente complejas, como la producción industrial o el análisis de radiografías en medicina, a través de programas de ordenador, que sustituyen la actividad humana (HOFFMAN-RIEM, W: *Big Data. Desafíos también para el Derecho,* Cizur Menor, Aranzadi, 2018, págs. 59 y ss).

Pero el ámbito de la IA va más allá. Destaca en este sentido el sistema de la denominada *"machine learning"*, definido en 1959 por Arthur Samuel como el campo de estudio que confiere a los ordenadores la habilidad de aprender sin ser explícitamente

programados. Esto significa un programa, que, una vez creado, es capaz de aprender cómo realizar actuaciones inteligentes fuera de la noción programada. Las ventajas de los algoritmos que emplean estos sistemas son obvias. En lugar de tener que crear un programa distinto para resolver cada problema individual, el algoritmo de la *"machine learning"* simplemente necesita aprender, a través de un proceso llamado *"training",* para resolver cada nuevo problema. De modo que los algoritmos inteligentes no se programan solo para resolver problemas específicos, sino también para aprender cómo resolver problemas (TUTT, A: "An FDA for algorithms", *Administrative Law Review* 83 (2017), ttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994, págs.. 1 y ss).

Este fenómeno se observa en particular en el área del llamado *"conocimiento profundo*" o *"redes neuronales artificiales*" (DNN, por sus siglas en inglés), que constituye una subcategoría de las "*machine learning*". El conocimiento o aprendizaje profundo es una parte de la inteligencia artificial, definida como la ciencia de crear sistemas inteligentes que tienen la habilidad de conseguir similares metas que los humanos. Estas redes neuronales son un subconjunto de algoritmos de aprendizaje automático que están inspiradas en las conexiones neuronales que se producen en el cerebro humano (VI V I 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), https://ieeexplore.ieee.org/document/8114708, pág. 2296). La referencia a las neuronas se explica porque se trata de sistemas que tratan de emular la actividad del cerebro humano – "*brain-inspired computation"*-, debido a que este se considera la mejor "máquina" para aprender y resolver problemas, por lo que es natural que se busque la aproximación al mismo.

En consecuencia, un *"brain-inspired computation*" es un programa que toma en cuenta algunos aspectos de la forma en que funciona el cerebro humano, al objeto de permitir que el sistema aprenda sin necesidad de intervención humana adicional; en particular es capaz de captar relaciones, estructuras y arquitecturas y de mejorar autónomamente su rendimiento. La capacidad de aprendizaje del sistema condiciona los procedimientos en tanto que es autónoma. Los pasos individuales como tales continúan controlados determinísticamente; pero existe un gran número de ellos y están relacionados entre sí de manera mucho más dinámica, de modo que es dificultoso, y, en muchos casos, prácticamente imposible, reconstruir la norma determinista. Tales programas, que dependen de la capacidad de aprendizaje, se utilizan, por ejemplo, en el procesamiento de imágenes y del habla, la robótica y la prognosis. En atención a ello, hay quien prefiere hablar de "*super software*", en lugar de hacerlo de IA.

Si bien no hay que descartar su dependencia del hardware. Aunque la AI está comúnmente asociada a los avances en *software,* lo cierto es que la ejecución y puesta en práctica de la misma depende en gran medida del *hardware*. Solo desarrollando *hardware* optimizado para los algoritmos de la AI se estima que está puede continuar evolucionando de forma sensible. Aunque los sistemas de AI también pueden mejorar la ejecución del *hardware.* Existe, pues, una reciprocidad entre ellos (The national artificial intelligence research and development strategic plan – USA 2016, págs. 21 y 22. Disponible en

https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf. En un sentido similar 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- Inteligencia artificial para Europa de 25 de abril de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES)

A grandes rasgos es posible, pues, coincidir en que existen tres tipos de IA (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). La IA o *narrow* IA, que es capaz de llevar a cabo tareas predefinidas. La *general* IA (IAGI), que puede llevar a cabo tareas intelectuales similares a las humanas. Y *super* IA (SIA) que, se dice, superará a la inteligencia humana en todos los aspectos; pero que, de momento, es poco más que ciencia ficción. Otros (BLANCO, JM/ COHEN, J. "Inteligencia artificial y poder", *ARI* (93) 2018, pág. 2) opinan, sin embargo, que, en realidad existen dos tipologías de IA. La que denominan "débil", ya existente, que comprende máquinas reactivas, que predicen en escenarios planteados, como Deep Blue, el programa de IBM que venció al ajedrez a Garry Kasparov; o la IA de memoria limitada, que utiliza experiencias pasadas para informar el futuro. En ella, los sistemas son entrenados para tareas muy concretas y se han incorporado a multitud de desarrollos tecnológicos como Siri en Apple. Sin embargo, la verdadera disrupción se producirá con la denominada IA "fuerte" por la disponibilidad de datos, el incremento de la capacidad de computación y la reducción de su coste, y la mejora de los algoritmos. Este avance acercará la IA a las habilidades cognitivas humanas de forma generalizada y el factor diferenciador será la capacidad de computación. Para ello, este tipo de IA se apoya en el *deep learning*, el *machine learning*, el procesamiento de lenguaje natural, el análisis predictivo, el reconocimiento de imagen y texto, la computación gestual, la realidad aumentada, la robótica y el reconocimiento emocional y, todo ello con el apoyo de la ciencia de datos.

Esta breve semblanza de los contornos de la IA permite comprender que la base de su funcionamiento reside en los algoritmos. Con carácter general se denomina algoritmo una sucesión finita de pasos no ambiguos que se pueden ejecutar en un tiempo finito, cuya razón de ser es la de resolver problemas. Por tanto, "problema" desde esta perspectiva es cualquier cuestión, conceptual o práctica, cuya solución es expresable mediante un algoritmo.

Ahora bien, los algoritmos existen al margen de la digitalización. De la misma forma, existen numerosas maneras de expresar un algoritmo, como, por ejemplo, una secuencia matemática o un diagrama de flujo. La especificidad de los algoritmos informáticos consiste en que, para poder usarlos en ordenadores, deben estar escritos en un lenguaje digital procesable mecánicamente. La fase de conversión de un algoritmo en instrucciones de un lenguaje de programación se denomina codificación. El código deberá estar escrito de acuerdo con la sintaxis del lenguaje de programación ya que solamente las instrucciones sintácticamente correctas pueden ser interpretadas por el

computador. Es lo que se denomina código fuente de programa. El código fuente de un programa informático o *software* es un conjunto de líneas de texto que expresa el cúmulo de instrucciones que debe seguir el ordenador para ejecutar el programa. Por tanto, en el código fuente del programa está escrito por completo su funcionamiento.

Sin embargo, este primer estadio no es directamente ejecutable por el ordenador. Debe ser traducido al lenguaje máquina o código objeto, también denominado código binario, debido a que funciona con listas de «1» y «0» de las que hay dos clases. La primera está compuesta por listas que sirven para darle instrucciones a la máquina (*software*), mientras que la segunda clase de listas está constituida por los datos que son procesados mediante la ejecución de las instrucciones. De esta manera, por ejemplo, una lista de «1» y «0» constituirá un programa de edición de textos, mientras que otra lista de «1» y «0» será una carta redactada utilizando el anterior programa. Análogamente, una lista de «1» y «0» puede ser un navegador de internet y la otra lista de «1» y «0» la página que se está visualizando, etc (DE LA CUEVA GONZÁLEZ-COTERA, J: "La importancia del código fuente", en *Derecho digital: retos y cuestiones actuales*, 2018, pág. 1). El procedimiento por el que se obtiene un código binario del código fuente se conoce como compilar. Todo ello en su conjunto constituye el programa informático o *software.*

Ahora bien, es preciso aclarar desde ahora que un mismo algoritmo puede ser expresado de diversas formas a través de un código informático, por lo que es posible que una misma secuencia de instrucciones se traduzca en varios programas de ordenador con unas funcionalidades similares y un código diferente. De otro lado, hay que tener en cuenta la peculiar relación que existe entre el código fuente y el código binario, puesto que de un código fuente puede obtenerse el código binario, pero del código binario no es posible obtener el código fuente, salvo en contadas excepciones. Disponer solamente de un código binario implica, por tanto, no conocer los elementos constitutivos de un programa de *software*, de modo que tampoco es factible saber cómo funciona realmente. Pudiera ser un software de edición de textos, pero pudiera contener un troyano (DE LA CUEVA GONZÁLEZ-COTERA,J: "La importancia del código fuente", cit., pág, 1).

Es conveniente, por otra parte, tener en cuenta la existencia de sectores conexos, que, aun cuando son imprescindibles para el funcionamiento de la IA, no forman parte de la misma en sentido estricto. En primer término cabe mencionar los datos. Los datos son el sustento de la IA, según expresa 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- de 7 de diciembre de 2018 (www.ipex.eu/IPEXL-WEB/dossier/files/.../082dbcc5679fb7b40167a1b3f76300c1.do).

Los desarrollos adicionales en materia de IA requieren un ecosistema de datos que funcione bien basado en la confianza, la disponibilidad de datos y la infraestructura. Para poder desarrollar la IA se precisan enormes cantidades de datos. El aprendizaje automático, que, según lo dicho, es un tipo de IA, consiste en la identificación de patrones en los datos disponibles y en la aplicación subsiguiente del conocimiento adquirido a nuevos datos. Cuanto más grande sea un conjunto de datos, mejor podrá la IA aprender y

descubrir incluso relaciones sutiles en los datos. 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.

Asimismo la capacidad informática es esencial para procesar los datos. La computación de alto rendimiento, las nuevas tecnologías de computación, almacenamiento y comunicación, y la inteligencia artificial deben entrelazarse cada vez más para que esta última consiga sus objetivos. 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), , sin olvidar el carácter instrumental que la tecnología *blockchain* desempeña en el marco de la IA. Buen ejemplo de ello constituyen los *smarts contracts*, que constituyen una manifestación de la IA, cuya eficacia ha sido mejorada por la tecnología *blockchain.*

II. EL DERECHO DE PATENTE SOBRE LA INTELIGENCIA ARTIFICIAL.

1. Planteamiento.

Conforme a su configuración, la patentabilidad de la IA ha de valorarse en un doble contexto. Por una lado, en el de los métodos matemáticos. Por otro, en el de las llamadas invenciones implementadas en ordenador. Una invención implementada en ordenador es aquella que implica el uso de un ordenador, una red informática u otro aparato programable en el que una o más de sus funciones se llevan a cabo total o parcialmente gracias a un programa de ordenador (EPO-Guidelines2018- GII. 3.6, disponible en https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_6.htm).

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 (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).

2. El carácter técnico.

Para que una creación del intelecto humano sea patentable se requiere, en primer término, que la misma constituya una invención, en el estricto sentido en que la Ley la concibe. Significa esto que la invención susceptible de ser patentada ha de ajustarse a la noción que la Ley acoge de la misma. La invención es, en ese preciso ámbito, una regla ideada para permitir la obtención de un resultado determinado de carácter técnico, que

puede referirse tanto al procedimiento como al objeto resultante. Ni el Convenio de Múnich sobre la concesión de patentes europeas de 1973 (en adelante CPE), ni la Ley 24/2015, de 24 de julio, de Patentes (en adelante, LP) suministran directamente esta definición, pero se infiere de los supuestos, que sí prevén, que no consideran invenciones.

No son, en efecto, invenciones los meros descubrimientos, ya que no suministran aquella regla, sino que se limitan a constatar elementos que ya existen en la naturaleza. Tampoco se consideran invenciones las obras literarias, artísticas o cualquier otra creación estética, así como los métodos matemáticos, las teorías científicas, los planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales, los programas de ordenadores o las formas de presentar informaciones (arts. 4.4 LP, y 52.2 CPE) debido a su naturaleza abstracta, y, por ende, a la ausencia de carácter técnico. Por tanto, el carácter técnico de una invención constituye un elemento inherente a la misma, sin el cual pierde la consideración de tal (por todo, BOTANA AGRA, M: "Invenciones patentables", en *Manual de la Propiedad Industrial,* Madrid, Marcial Pons, 2009, págs.., 107 y ss., 109). El carácter técnico es un requisito implícito que debe reunir una creación para que sea considerada invención en el sentido de los artículos 4.1 LP y 52 CPE.

El hecho, en resumen, de que la protección mediante patente quede reservada a las creaciones técnicas ha formado parte de la tradición jurídica europea desde los primeros días del sistema de patentes. En consecuencia, el objeto para el cual se busca protección debe tener carácter técnico o, para ser más precisos, debe incluir una enseñanza técnica, es decir, una instrucción dirigida a un experto técnico sobre cómo resolver un problema técnico particular (antes que, por ejemplo, un problema financiero, comercial o matemático) mediante el uso de medios técnicos particulares.

Los preceptos citados excluyen en concreto la consideración de invención tanto de los métodos matemáticos, como de los programas de ordenador, que, según lo indicado antes, constituyen los dos soportes de la IA. Recuérdese que la IA está basada en métodos computacionales que utilizan algoritmos, y, por tanto, las invenciones relativas a la misma se clasificarían bien como simples programas de ordenador o bien como meros programas de naturaleza matemática abstracta, constitutivos de métodos abstractos privados de carácter técnico. Esto implica que, por sí sola, la IA no cumple los requisitos de patentabilidad.

En este sentido se pronuncian la Directrices de examen de la Oficina Europea de Patentes 2018 (en adelante, EPO, por sus siglas en inglés). Las Directrices disponen que la inteligencia artificial se basa en modelos computacionales y algoritmos para la clasificación, agrupación, regresión y reducción de la dimensionalidad, tales como redes neuronales, algoritmos genéticos, máquinas de vectores de soporte, k-medias, regresión del núcleo y análisis discriminante y que dichos modelos computacionales y algoritmos son *per se* de naturaleza matemática abstracta. En atención a ello, concluye que la patentabilidad de la misma debe ser analizada en el contexto de las Directrices relativas a los métodos matemáticos. De hecho, las especificaciones que se contienen en ellas en relación con la IA constituyen un subapartado de los "métodos matemáticos", incluidas en la parte "G" (patentabilidad), dentro de la lista de exclusiones.

Ahora bien, tanto el artículo 52.3 del CPE, como el artículo 4.5 de la LP, anudan la exclusión de patentabilidad de las actividades o materias anteriores *"solamente en la medida en que la solicitud de patente o la patente se refiera exclusivamente a una de ellas considerada como tal"*.

Según declara la Decisión de la Cámara de Recursos de la EPO T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998 la combinación de las dos disposiciones contenidas en los apartados 2 y 3 del CPE demuestra que el CPE no quiso excluir de la patentabilidad todas las materias o actividades relacionadas en el apartado 2. Estima asimismo que tanto la naturaleza de excepciones de la lista de exclusiones de patentabilidad, prevista en el artículo 52.2 CPE, como la disposición contenida en el artículo 52.3 CPE, obligan a concluir que el alcance de dichas exclusiones no puede ser interpretada de manera amplia. En otras palabras, el hecho de que solo las solicitudes de patente relacionadas con programas para computadoras (o con métodos matemáticos) como tales estén excluidas de la patentabilidad significa que es posible patentar creaciones relacionadas con programas para computadoras (o para métodos matemáticos), siempre que no se consideran programas para computadoras (o métodos matemáticos) como tales.

La interpretación del significado del inciso "*como tal*" – *as such*- se torna entonces esencial para decidir en torno a la patentabilidad de ambos. Basándose en que la exclusión de la patentabilidad de los programas para computadoras como tales puede interpretarse en el sentido de que dichos programas se consideran meras creaciones abstractas, que carecen de carácter técnico, debido al uso de la expresión *"no se considerará como invenciones"* y a que, en el contexto de la aplicación del CEP, el carácter técnico de una invención se acepta generalmente como un requisito esencial para su patentabilidad, según hay que deducir de las Reglas 42 y 43 -contenido de la descripción y forma y contenido de las reivindicaciones- del Reglamento de Ejecución del Convenio relativo a la patente europea, la Decisión de la Cámara de Recursos de la EPO T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998 , concluyó que el inciso *"como tal"* debe ser interpretado en el sentido de que el programa en cuestión carezca de carácter técnico, por lo que el mismo debe considerarse como invención patentable cuando tenga un carácter técnico.

La dificultad reside, por tanto, en determinar qué debe entenderse por carácter técnico. Sin embargo, tal y como exponen las Directrices de examen de solicitudes de patente elaboradas por la Oficina española de Patentes y Marcas (en adelante OEPM), al igual que no existe una definición de invención, los textos legales tampoco se pronuncian sobre qué debe entenderse por carácter técnico, lo que, por lo demás, se considera inconveniente. Una definición de dicho carácter podría provocar una barrera infranqueable para que algunos avances en determinados campos de la tecnología pudieran acceder a la protección otorgada por las patentes o exigir una constante revisión de dicha definición. Por otra parte, el alcance del significado de la palabra *"técnica"* está en cierta medida condicionado por el contenido global del estado de la técnica. Elementos o actividades que hace un tiempo no se consideraban materias técnicas, hoy en día sí lo son. Por ejemplo, la traducción de idiomas era una actividad exclusivamente realizada

por seres humanos. Actualmente, sin embargo, esta tarea se puede llevar a cabo por máquinas lo que, en algunos casos, da lugar a que este procedimiento de traducción se convierta en una actividad técnica. Lo mismo puede aplicarse al reconocimiento automático de la voz o de la imagen de personas. Esta traslación de elementos desde el terreno de las materias desprovistas de carácter técnico al ámbito de la técnica es consecuencia justamente de la divulgación de desarrollos tecnológicos que permiten extraer una determinada actividad del entorno de lo exclusivamente humano e incorporarla al campo de la tecnología.

De modo que resulta necesario delimitar el alcance del carácter técnico en atención a los grupos de casos que se advierten en la práctica. A este respecto es obligado atender a las Directrices de examen de la EPO sobre inteligencia artificial. El hecho, no obstante, de que sean estas especialmente limitadas aconseja completar sus indicaciones con las previstas, en general, para los métodos matemáticos y para las invenciones implementadas por ordenador. Junto a ello es preciso considerar las decisiones de las Cámaras de Recurso de la EPO y la práctica que, según ellas, sigue dicha Oficina, porque precisamente este organismo internacional tiene la responsabilidad de decidir sobre la petición de patentes dentro del sistema del CEP y las Cámaras desempeñan un poder judicial independiente en ese sistema, en cuyo marco son competentes para revisar las decisiones tomadas por la EPO en procedimientos de concesión y oposición. Esta opción resulta asimismo útil en el contexto interno puesto que la práctica de examen de este tipo de invenciones seguida por la OEPM es esencialmente la misma que la aplicada por la EPO.

Conforme a ello es posible coincidir en que el carácter técnico de la IA puede consistir tanto en el hecho de su aplicación a un campo de la tecnología, como en su adaptación a una implementación técnica específica (LIEVENS, K: *Patenting Artificial Intelligence,* cit. Y vid. Directrices de examen EPO G-II, 3.3 –métodos matemáticos- y 3.3.1 -Inteligencia artificial y aprendizaje automático-).

El carácter técnico puede residir, en efecto, en la aplicación de la IA en un determinado campo tecnológico. Dicha aplicación requiere en primer término que el modelo computacional en que consiste tenga un *propósito técnico*. Resolviendo en torno a un método de clasificación automática de registros de datos, la Decisión de la Sala de Recursos EPO T 1784/06 (Método de clasificación / COMPTEL) de 21.9.2012 (ECLI: EP: BA: 2012: T178406.20120921) declara que, dado que el algoritmo en que se basa es un método matemático y los métodos matemáticos como tales no se consideran invenciones, el carácter técnico del algoritmo podría reconocerse solo si tiene una finalidad técnica, lo que no se aprecia en el caso puesto que la clasificación automática de registros de datos reivindicada sirve únicamente para clasificar los registros de datos, sin que ello implique ningún uso técnico de la clasificación, sino usos no técnicos, administrativos o comerciales, de los registros de datos clasificados. A la luz de la descripción, el método de clasificación prepara los procedimientos de calificación y facturación. Por lo tanto, la Junta no considera el resultado del algoritmo, un conjunto de registros de datos clasificados, como técnico.

El propósito técnico, además, ha de ser *específico*. Un propósito genérico no es suficiente para conferir carácter técnico. Pronunciándose acerca de una reivindicación que definía un método para clasificar documentos de texto esencialmente en términos de un algoritmo matemático abstracto, que debía ser ejecutado por una computadora, pero solo refiriéndose a los pasos del método como "informatizados" y a los documentos de texto como "digitalmente representados en una computadora", la Decisión de la Sala de Recursos EPO T 1358/09 (Clasificación / BDGB SOFTWARE EMPRESARIAL) de 21.11.2014 (ECLI: EP: BA: 2014: T135809.20141121) determinó que un algoritmo matemático contribuye al carácter técnico de un método implementado por computadora solo en la medida en que cumple un propósito técnico, lo que no se advirtió en el caso puesto que el algoritmo servía solo para el propósito general de clasificar documentos de texto y la clasificación de los documentos de texto es ciertamente útil, ya que puede ayudar a localizar documentos de texto con un contenido cognitivo relevante, pero no puede ser considerado como un propósito técnico. El hecho de que dos documentos de texto con respecto a su contenido textual pertenezcan a la misma "clase" de documentos no constituye un problema técnico.

En este mismo sentido se pronunció la Decisión de la Sala de Recursos EPO T 1316/09 de 18.12.2012 (ECLI: EP: BA: 2012: T131609.20121218) estimando que los métodos de clasificación de textos en sí no produjeron un efecto técnico relevante ni proporcionaron una solución técnica a ningún problema técnico. La clasificación del texto en sí no tiene ningún propósito técnico. La combinación de diferentes métodos de categorización de texto tampoco proporciona ningún efecto técnico relevante que pueda constituir una base válida para definir el problema técnico objetivo.

Según especifica la Decisión de la Cámara de Recursos EPO T 1227/05 (Simulación de circuito I / Infineon Technologies) de 13.12.2006 (ECLI: EP: BA: 2006: T122705.20061213) es preciso además que el método reivindicado esté funcionalmente limitado a ese propósito técnico, lo que requiere establecer un vínculo suficiente entre el propósito técnico y los pasos del modelo. En el caso, el propósito declarado, la simulación de un circuito sujeto a 1 / f de ruido, se establece en las etapas adicionales del método reivindicado. Sobre la base de la derivación física y matemática especificada en la descripción, es verificable que los números aleatorios generados de acuerdo con las reivindicaciones introducen realmente 1 / f de ruido en la simulación del circuito. Por este motivo, la Sala estima que las reclamaciones del método independiente se limitan funcionalmente a la simulación de un circuito afectado por ruido. La simulación realiza funciones técnicas típicas del trabajo de ingeniería moderna. Proporciona una predicción realista del rendimiento de un circuito diseñado y, por lo tanto, idealmente permite que se desarrolle de manera tan precisa que las posibilidades de éxito de un prototipo puedan evaluarse antes de que se construya.

En definitiva, el que el modelo sirva para un propósito técnico está determinado principalmente por la relevancia técnica directa de los resultados que proporciona. Entre los ejemplos de eventuales aplicaciones técnicas de los algoritmos insertos en el modelo computacional se cita el uso de una red neuronal en un aparato de monitoreo cardíaco con el propósito de identificar latidos cardíacos irregulares; así como la clasificación de imágenes digitales, videos, señales de audio o voz basadas en características de bajo nivel (v.gr., bordes o atributos de píxeles para imágenes). La detección de fallos y el mantenimiento predictivo, el análisis médico o los automóviles auto-conducibles son otros ejemplos de la misma índole. Sin embargo, como se ha indicado antes, no se considera que la clasificación de documentos de texto únicamente con respecto a su contenido textual sea *per se* un propósito técnico sino lingüístico (Decisiones T 1358/09 y T 1316/09). La clasificación de registros de datos abstractos o incluso "registros de datos de redes de telecomunicación" sin ninguna indicación de que se haga un uso técnico de la clasificación resultante tampoco es *per se* un propósito técnico, incluso si se considera que el algoritmo de clasificación tiene propiedades matemáticas valiosas, como la solidez, lo que implicaría beneficios técnicos si se utilizara para un propósito técnico. Sin embargo, la reivindicación en cuestión no se limita a ninguna aplicación técnica de su método de clasificación. De acuerdo con la descripción, los registros de datos se clasifican con el propósito no técnico de facturación (Decisión T 1784/06).

Independientemente de cualquier aplicación técnica, el carácter técnico de la IA puede derivar, en segundo lugar, del hecho de que el modelo computacional y los algoritmos en que se basa estén especialmente diseñados y adaptados para *una implementación técnica específica* o a que su diseño esté motivado por *consideraciones técnicas sobre el funcionamiento interno del ordenador* (Decisión de la Junta Ampliada EPO G 0003/08 (Programas para ordenadores) del 12.5.2010 (ECLI: EP: BA: 2010: G000308.20100512) y Decisión de la Cámara de recursos EPO 1358/09 (Clasificación / BDGB SOFTWARE EMPRESARIAL) de 21.11.2014, ECLI: EP: BA: 2014: T135809.20141121). Por tanto, no será suficiente una implementación técnica genérica, ni un algoritmo que es supuestamente más eficiente que uno anterior, ni una mera programación.

La Decisión de la Cámara de recursos EPO T 1358/09 (Clasificación / BDGB SOFTWARE EMPRESARIAL) de 21.11.2014, ECLI: EP: BA: 2014: T135809.20141121 parte de la consideración de que si un algoritmo es particularmente adecuado para ser ejecutado en una computadora, ya que su diseño fue motivado por consideraciones técnicas del funcionamiento interno de la computadora, se le podría atribuir carácter técnico. Cita a este respecto la Decisión T 258/03, (Método de subasta / HITACHI) de 21.4.2004, **(**ECLI: EP: BA: 2004: T025803.2004042**).** En esta Decisión la Cámara de recursos sostiene que si un paso de un método ha sido diseñado de tal manera que sea particularmente adecuado para ser realizado en una computadora, podría decirse que tiene un carácter técnico, debido a que un paso de este tipo requiere consideraciones técnicas, a saber, los principios de funcionamiento de una computadora. Se examinaba en el caso un método de subasta en soporte informático al que se atribuyó carácter técnico en razón de que el programa informático diseñado incluía una forma de clasificar las ofertas consistente en aumentar el precio de la subasta sucesivamente para determinar el precio máximo más alto ofrecido por los oferentes que propusieron el mismo precio deseado, y dicha característica constituye una solución técnica a un problema. Sin embargo, la patente fue denegada por falta de actividad inventiva debido a que dicha forma de clasificar las ofertas se consideró una medida de programación rutinaria al alcance de las personas expertas. En definitiva, aunque se aceptó que esa característica, constituía una solución técnica a un problema, habría sido evidente para los expertos en la materia de procesamiento de datos.

A pesar de que, según lo dicho, la Decisión T 1358/09, dice basarse en esta última Decisión, se aparta de la misma, puesto que no considera suficiente para atribuir carácter técnico la simple búsqueda de un algoritmo informático para llevar a cabo algún procedimiento. Declara que el algoritmo que subyace al método de la reivindicación no va más allá de una formulación matemática particular de la tarea de clasificar documentos. El objetivo de esta formulación es claramente permitir que una computadora lleve a cabo esta tarea, pero no se puede reconocer otra consideración del funcionamiento interno de una computadora, razón por la que concluye en que no existen consideraciones técnicas relevantes, ya que tales consideraciones técnicas deben ir más allá de la determinación del algoritmo informático idóneo para realizar la tarea.

Se basa para ello en la Decisión G 0003/08 (Programas para ordenadores) del 12.5.2010 (ECLI: EP: BA: 2010: G000308.20100512). En opinión de Junta Ampliada, de donde procede esta Decisión, la actividad de definición de un algoritmo de computadora puede ser aprehendida desde dos puntos de vista diferentes. Por un lado, es posible catalogarla como un ejercicio matemático-lógico puro; por otro lado, como la definición de un procedimiento para hacer que una máquina realice una determinada tarea. Dependiendo de cuál de estas dos perspectivas se tenga en cuenta, la pregunta de si la programación de computadora siempre implica "consideraciones técnicas" puede responderse de manera negativa o positiva. Aparentemente, cualquiera de los dos puntos de vista puede sostenerse genuinamente, sin embargo, en opinión de la Junta, la intención de los redactores del CEP fue adoptar una opinión negativa, es decir, considerar la formulación abstracta de algoritmos como no perteneciente a un campo técnico.

Por otra parte, añade que, aunque se puede decir que toda la programación informática implica consideraciones técnicas, ya que se refiere a la definición de un método que puede realizar una máquina, esta consideración no es en sí misma es suficiente para demostrar que el programa resultante de la programación tiene un carácter técnico. Por el contrario, se requieren, *"consideraciones técnicas adicionales"* que van más allá de *"simplemente"* encontrar un algoritmo de computadora para realizar una tarea.

La Decisión justifica esta conclusión en la aplicación al caso de un razonamiento similar al utilizado en la Decisión de la Cámara de Recursos EPO T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998 (ECLI:EP:BA:1998:T117397.19980701. La Decisión T 1173/97 establece la noción de *"efecto técnico adicional"*. Declara que no es posible considerar que los programas para computadoras tengan un carácter técnico por el mero hecho de que sean programas para computadoras, lo que, a su juicio, significa que las modificaciones físicas del *hardware* (que causan, por ejemplo, corrientes eléctricas) derivadas de la ejecución de las instrucciones dadas por los programas para computadoras no pueden constituir el carácter técnico requerido para evitar la exclusión de dichos programas. Aunque tales modificaciones pueden considerarse técnicas, son una característica común de todos aquellos programas para computadoras que se han hecho adecuadas para ejecutarse en una computadora y, por lo tanto, no pueden usarse para distinguir programas para computadoras con un carácter técnico de programas para computadoras como tales.

El carácter técnico ha de hacerse residir, por tanto, en los "*efectos técnicos adicionales"* derivados de la ejecución (por el *hardware*) de las instrucciones dadas por el programa de computadora. Un efecto técnico de ese tipo se logra mediante el funcionamiento interno de una computadora bajo la influencia de dicho programa, esto es, también puede ser causado por el funcionamiento de la computadora en la que se ejecuta el programa, es decir, por el funcionamiento del *hardware* de esa computadora, siempre y cuando las modificaciones físicas del *hardware* que se derivan de la ejecución de las instrucciones dadas por el programa sean distintas a las modificaciones físicas *"normales"* del mismo (que causan, por ejemplo, corrientes eléctricas) derivadas de la ejecución de las instrucciones dadas por los programas para computadoras. Cuando dichos efectos adicionales tienen un carácter técnico o cuando el *software* resuelve un problema técnico, una invención que produce tal efecto puede considerarse una invención que, en principio, puede ser el objeto de una patente.

En opinión de la Sala, es posible, por tanto, conceder una patente no solo en el caso de una invención en la que una pieza de *software* gestiona, mediante una computadora, un proceso industrial o el funcionamiento de una pieza de maquinaria, esto es, un proceso técnico, sino también en todos aquellos casos en que un programa de computadora es el único medio, o uno de los necesarios, de obtener *"un efecto técnico adicional"* en el sentido indicado anteriormente.

Ahora bien el *"efecto técnico adicional"* puede ser "*potencial"*. Al respecto la Decisión comentada explica que cada producto de programa de computadora produce un efecto cuando el programa en cuestión está hecho para ejecutarse en una

computadora. Sin embargo, el efecto solo se muestra en la realidad física cuando el programa se está ejecutando. Por lo tanto, el producto del programa informático en sí mismo no revela directamente dicho efecto en la realidad física. Solo revela el efecto cuando se está ejecutando y, en consecuencia, solo posee el *"potencial"* para producir dicho efecto. Por lo tanto, un producto de programa informático puede poseer un carácter técnico porque tiene el potencial de causar un efecto técnico adicional predeterminado en el sentido anterior.

En definitiva, en opinión de la Sala, un programa informático reivindicado por sí mismo no se excluye de la patentabilidad si el programa, cuando se ejecuta en una computadora o se carga en una computadora, produce, o es capaz de producir, un efecto técnico que va más allá del interacciones físicas "normales" entre el programa (*software*) y la computadora (*hardware*) en la que se ejecuta. "Ejecutar en una computadora" significa que el sistema que comprende el programa de computadora más la computadora lleva a cabo un método (o proceso) que puede ser un método para la recuperación de recursos en un sistema informático (reclamación de método o reclamación de proceso). "Cargado en una computadora" significa que la computadora programada de esta manera es capaz o está adaptado para llevar a cabo el método anterior y por lo tanto constituye un sistema (o dispositivo o aparato) que puede ser objeto de una reivindicación de un sistema informático (reivindicación de aparato o reivindicación de dispositivo) para llevar a cabo el método de la reivindicación anterior.

Sobre la base de esta distinción, la Decisión G 0003/08 (Programas para ordenadores) del 12.5.2010 (ECLI: EP: BA: 2010: G000308.20100512) concluye, según lo dicho, en que la simple búsqueda de un algoritmo informático para llevar a cabo algún procedimiento no supone una "*consideración técnica"* en el sentido requerido por el CEP , ni, por ende, es apta para fundamentar el carácter técnico de la creación, ni para demostrar que el programa resultante de la programación tiene un carácter técnico. Por el contrario, se requieren, *"consideraciones técnicas adicionales"* que van más allá de *"simplemente"* encontrar dicho algoritmo. Estas consideraciones técnicas adicionales deben reflejarse en las características reivindicadas que causan un efecto técnico adicional.

Supuestos de efectos técnicos adicionales que confieren carácter técnico a los programas informáticos son el control de un proceso técnico o del funcionamiento interno de la computadora o sus interfaces (Directrices EPO G-II, 3.6.1). El control de un proceso técnico se produce, por ejemplo, en un programa de computadora que especifica un método para controlar un sistema de frenos antibloqueo en un automóvil, determinar las emisiones de un dispositivo de rayos X, comprimir video, restaurar una imagen digital distorsionada o cifrar las comunicaciones electrónicas. Ejemplos de programas de computadora que controlan el funcionamiento interno o la operación de una computadora o de sus interfaces pueden ser el balanceo de carga del procesador o la asignación de memoria.

Hipótesis de programas de computadora diseñados sobre la base de consideraciones técnicas específicas del funcionamiento interno de la computadora en la

que se ejecutará, por ejemplo, al estar adaptado a la arquitectura específica de la computadora, son los programas informáticos que implementan medidas de seguridad para proteger la integridad del arranque o las contramedidas contra los ataques de análisis de potencia tienen un carácter técnico, ya que se basan en una comprensión técnica del funcionamiento interno de la computadora (Directrices EPO G-II, 3.6.1). Constituye también una "*consideración técnica adicional",* por ejemplo, la adaptación de un algoritmo de reducción polinomial para explotar los cambios de tamaño de palabra que coinciden con el tamaño de palabra del hardware de la computadora se basa en tales consideraciones técnicas y puede contribuir a producir el efecto técnico de una implementación de hardware eficiente de dicho algoritmo. Sin embargo, incluir una red de auto-clasificación de datos en un sistema de telecomunicaciones, a pesar de poder tener unos nuevos algoritmos que mejoran y dan robustez al modelo, no permiten obtener un efecto técnico que no sea puramente matemático.

En cualquier caso, es importante retener que, una vez constatado el abandono del llamado *"enfoque de la contribución"*, que exigía determinar la contribución técnica que logra una invención con respecto al estado de la técnica para apreciar el carácter técnico, la presencia de un efecto técnico adicional y, por tanto, del carácter técnico, se evalúa sin hacer referencia al estado de la técnica. De ello se deducen dos consideraciones de la máxima importancia. Por un lado, que la determinación de si un programa de computadora está excluido o no de la patentabilidad conforme a los artículos 52.2 y 3 CEP es independiente del estado de la técnica. Es decir, el efecto técnico adicional identificado no necesita ser nuevo. Este aspecto solo puede ser considerado al examinar la concurrencia de los requisitos de patentabilidad atinentes a la novedad y a la actividad inventiva.

Y, en segundo lugar, en el lado inverso, que aspectos que puedan considerarse novedosos, si carecen de carácter técnico no justifican por sí solos la presencia de un efecto técnico adicional. Son los casos, por ejemplo, de programas informáticos para un propósito no técnico que requieran menos tiempo de computación que un programa de la técnica anterior que tenga el mismo propósito no técnico, (entre más, Decisión T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998, ECLI:EP:BA:1998:T117397.19980701, Decisión T 1227/05 (Simulación de circuito I / Infineon Technologies) de 13.12.2006 ,ECLI: EP: BA: 2006: T122705.20061213, Decisión G 0003/08 (Programas para ordenadores) del 12.5.2010, ECLI: EP: BA: 2010: G000308.20100512, Decisión T 1784/06 (Método de clasificación / COMPTEL) de 21.9.2012, ECLI: EP: BA: 2012: T178406.20120921, Decisión de la Sala de Recursos EPO T 1370/11 (Sistema de propiedad a demanda / MICROSOFT) del 11.3.2016 ECLI: EP: BA: 2016: T137011.20160311) Del mismo modo, comparar un programa de computadora con la forma en que un ser humano realizaría la misma tarea no es una base adecuada para evaluar si el programa de computadora tiene un carácter técnico (Decisión de la Sala de Recursos EPO T 1358/09 (Clasificación / BDGB SOFTWARE EMPRESARIAL) de 21.11.2014 ECLI: EP: BA: 2014: T135809.20141121).

Con todo, la jurisprudencia de las Salas de Recurso EPO dista de ser lo suficientemente homogénea y estable. En particular resulta ambigua en un grado no

irrelevante cuando analiza los programas informáticos y los métodos implementados en un sistema informático. Citando las conclusiones alcanzadas en las Decisiones T 0258/03 (Método de subasta / HITACHI) de 21.4.2004 **(**ECLI: EP: BA: 2004: T025803.2004042**) ,** T 424/03 (formatos de Portapapeles I / MICROSOFT) de 23.2.2006 (ECLI: EP: BA: 2006: T042403.20060223) y G 0003/08 (Programas para ordenadores) del 12.5.2010 (ECLI: EP: BA: 2010: G000308.20100512), (Directrices de examen EPO G-II, 3.6 - Programas para computadoras), - exponen que se hace necesario distinguir entre el programa informático o *software* en sí mismo considerado y el método implementado en un sistema informático. Según las citadas Directrices, el primero se refiere a una secuencia de instrucciones ejecutables por computadora que especifican un método, mientras que el último se refiere a un método que se realiza realmente en una computadora. En atención a ello, concluye que las reclamaciones relativas a un método implementado por computadora, un medio de almacenamiento legible por computadora o un dispositivo no pueden objetarse por carecer de carácter técnico, ya que se trata de un método que implica el uso de medios técnicos (por ejemplo, una computadora) y cualquier medio técnico en sí mismo (por ejemplo, una computadora o un medio de almacenamiento legible por computadora) tiene carácter técnico y, por lo tanto, representa una invención en el sentido de artículo 52.1 CEP.

La Decisión de la Sala de Recursos EPO T 424/03 (formatos de Portapapeles I / MICROSOFT) de 23.2.2006 (ECLI: EP: BA: 2006: T042403.20060223), declara a ese respecto que un método implementado en un sistema informático representa una secuencia de pasos realmente realizados y que logra un efecto, y no una secuencia de instrucciones ejecutables por computadora (es decir, un programa informático) que solo tiene el potencial de lograr tal efecto cuando se carga y se ejecuta en la computadora. Por lo tanto sostiene que la categoría de reclamación de un método implementado por computadora se distingue de la de un programa de computadora. Aunque un método, en particular un método para operar una computadora, puede ponerse en práctica con la ayuda de un programa informático, una reclamación relacionada con dicho método no reclama un programa informático en la categoría de un programa informático como tal, sino un método implementado en un sistema informático. Un sistema informático que incluye una memoria (portapapeles) es un medio técnico y, en consecuencia, el método reivindicado tiene carácter técnico de acuerdo con la jurisprudencia establecida.

Por otro lado, la Decisión también considera los pasos del método reivindicado para contribuir al carácter técnico de la invención. Estos pasos resuelven un problema técnico por medios técnicos, ya que las estructuras de datos funcionales (formatos de portapapeles) se usan independientemente de cualquier contenido cognitivo (ver T 1194/97 - Producto de estructura de datos / Philips; OJ EPO 2000, 525) para mejorar la capacidad interna y el funcionamiento de un sistema informático con el fin de facilitar el intercambio de datos entre diversos programas de aplicación. Por lo tanto, los pasos reivindicados proporcionan una computadora de propósito general con una funcionalidad adicional: la computadora ayuda al usuario a transferir datos que no están en archivos a archivos. En un sentido semejante la Decisión T 0258/03 (Método de subasta / HITACHI) de 21.4.2004 **(**ECLI: EP: BA: 2004: T025803.2004042**)** concluyó que, en general, un método que implica medios técnicos es una invención en el sentido del artículo 52. 1 CPE.

Al respecto es conveniente citar la Decisión G 0003/08 (Programas para ordenadores) del 12.5.2010 (ECLI: EP: BA: 2010: G000308.20100512), dictada por la Alta Cámara de Recursos (Junta de Apelación Ampliada). Esta Cámara tiene asignada la función de asegurar una aplicación uniforme del CPE bajo las condiciones definidas de manera estricta en el artículo 112.1 del mismo. Por lo tanto no constituye una instancia adicional que se ubique por encima de las Salas de Recurso dentro del sistema judicial del CPE, sino que solo interviene cuando existen divergencias entre las Decisiones de las Salas de Recurso técnicas que afecten a la citada aplicación uniforme. En este contexto, la Decisión G 0003/08 constituye la respuesta de la Alta Cámara a las cuestiones de derecho que le fueron sometidas a consideración por el Presidente de la OEP en torno al tratamiento poco claro o incluso incorrecto que estimaba se estaba dando a las invenciones implementadas en ordenador por las Salas de Recurso técnicas.

En ese contexto, la Decisión G 0003/08 (Programas para ordenadores) del 12.5.2010 (ECLI: EP: BA: 2010: G000308.20100512), reconoce que la Decisión T 424/03 (formatos de Portapapeles I / MICROSOFT) de 23.2.2006 (ECLI: EP: BA: 2006: T042403.20060223) se desvía de la opinión expresada en la Decisión T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998 (ECLI:EP:BA:1998:T117397.19980701), pero aduce que esto no es más que desarrollo legítimo de la jurisprudencia. La Decisión G 0003/08 se refiere en particular a que según la Decisión T 1173/97 para valorar las exclusiones en virtud del artículo 52. 2 y 3 CPE, no se hace ninguna diferencia acerca de si un programa de computadora es reclamado por sí mismo o como un registro en un proveedor, es decir, en un medio legible por computadora, de modo que el carácter técnico de ambos exigiría demostrar la existencia de "*efectos técnicos adicionales"* o efectuar *"consideraciones técnicas adicionales"*. Por el contrario, según la Decisión T 424/03 los requisitos aplicables a cada uno son distintos, de modo que los efectos o consideraciones adicionales solo resultan necesarios para demostrar el carácter técnico de los programas, pero no de los métodos que implementan los programas en el sistema informático.

Según la Decisión G 0003/08 esta última es la que debe considerarse como la posición actual de la jurisprudencia, de modo que, concluye, que una reclamación en el área de programas de computadora puede evitar la exclusión según los Artículos 52. 2 (c) y 52.3 CPE simplemente mencionando explícitamente el uso de una computadora o un medio de almacenamiento legible por computadora. Añade que no existen riesgos de divergencia puesto que la Decisión T 1173/97 no ha sido seguida en este punto por ninguna otra Decisión posterior. Sin embargo, tal vez sucediera eso en el momento en que se dictó la Decisión G 0003/08, pero no creo que pueda decirse lo mismo hoy a la vista, por ejemplo, de la Decisión de la Sala de Recursos EPO T 1370/11 (Sistema de propiedad a demanda / MICROSOFT) del 11.3.2016 (ECLI: EP: BA: 2016: T137011.20160311), que somete a ambos al mismo tratamiento. Declara, en efecto, que para que un método implementado por computadora o un programa de computadora sea patentable, se debe establecer que tiene un efecto técnico "adicional" y resuelve un problema técnico independientemente de su tiempo de computación absoluto o relativo. Solo entonces, estima, y solo si la supuesta aceleración afecta a un efecto técnico establecido, se puede argumentar que la aceleración contribuye a un efecto técnico.

III. LA COMPATIBILIDAD DEL SISTEMA DE PROTECCIÓN MEDIANTE PATENTE CON OTROS SISTEMAS DE PROTECCIÓN. EL DERECHO DE AUTOR Y LOS SECRETOS EMPRESARIALES.

La tutela de los programas de ordenador a través del derecho de autor constituye la forma tradicional y ordinaria de protección. Se basa en la afirmación 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". En el mismo sentido se pronuncia el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, adoptado en el seno de Organización Mundial del Comercio en 1994 (en adelante, ADPIC), cuyo artículo 10.1 señala que "los programas de ordenador, sean programas fuente o programas objeto, serán protegidos como obras literarias en virtud del Convenio de Berna" y el Tratado de la Organización Mundial de la Propiedad Intelectual (en adelante, OMPI) sobre Derecho de Autor adoptado en Ginebra en 1996, cuyo artículo 4 dispone que "los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el artículo 2 del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión".

Entre las ventajas que se citan a favor de esta forma de protección destacan su flexibilidad y su bajo coste. El derecho de autor protege el programa desde su creación, sin necesidad de registro, ni de otras formalidades. Además, para ser una obra protegida por derecho de autor debe cumplir únicamente el requisito de la originalidad, condición mucho más fácil de cumplir que los requisitos de patentabilidad. En consecuencia, la protección se abarata en gran medida, también porque se hace innecesaria la renovación de la protección por patente y el pago de un canon cada año. A cambio concede al titular el derecho exclusivo de uso en lo relativo a su reproducción, modificación y distribución, permitiéndole limitar o definir el acceso de terceros al mismo.

Entre los inconvenientes se aduce que se trata de una protección imperfecta, incompleta y obsoleta. Es imperfecta porque el derecho de autor puede ser fácilmente desconocido con el método del "*blind room*". Aunque un programa de ordenador guarde grandes similitudes con otro anterior no se considera plagio si el autor puede demostrar que su creación es independiente de la primera. El "*blind room"* permite a los programadores obtener una creación independiente. Un equipo examina el programa del competidor y lo transmite y un segundo equipo lo desarrolla como nuevo producto aunque basado en los resultados del primero. Este obstáculo se salva, no obstante, en el contexto del derecho de patente porque la infracción del derecho de exclusiva que otorga no requiere la existencia de copia. En este sentido las patentes pueden ser una forma poderosa de protección para la propiedad intelectual relacionada con
la IA, particularmente porque la creación independiente no es una defensa contra la infracción de patentes.

Se estima también que este sistema es incompleto, pues como bien ha puesto de manifiesto la Sentencia del TJUE de 3 de julio de 2012 (asunto C-128/11), la regulación prevista en relación con los actos de explotación contemplados respecto de los programas de ordenador no se adecúa a la nueva realidad tecnológica donde, en la gran mayoría de los casos, el programa de ordenador es distribuido mediante una descarga online del mismo. Por último, se observa el régimen es obsoleto puesto que está diseñado básicamente pensando en las licencias clásicas de usuario en relación con el *software* privativo, cuando la realidad muestra la irrupción cada vez mayor de las licencias de *software* libre, en cuyo contexto los programas de ordenador se acompañan de la autorización para que cualquiera pueda utilizarlos, copiarlos y distribuirlos, ya sea de

forma literal o con modificaciones, gratis o bien mediante una gratificación y en todo caso, estando disponible su código fuente (por todo, FERNÁNDEZ MASIÁ., E: "Programas de ordenador", en AA.VV: *Comentarios a la Ley de Propiedad intelectual*, dir. PALAU RAMÍREZ, F/PALAO MORENO, G, Valencia, Tirant lo Blanch, 2018, versión e-book, págs. 1183 y ss., 1194).

Sin embargo, el debate real entre una y otra forma de protección trasciende a las cuestiones jurídicas. Se trata de un debate económico que, en ocasiones, trata de disfrazarse como social, utilizándose todo tipo de argumentos emocionales, de tinte populista. Por un lado, los colectivos, en muchos casos relacionados con el desarrollo del *software* libre, como Linux, MySQL, PHP, se oponen a la patentabilidad del *software* aunque forme parte de una invención, aduciendo que frena la innovación y el desarrollo y sólo beneficia a las grandes multinacionales, perjudicando a las PYMES del sector. Por otro lado se alzan los defensores de la patentabilidad, entre ellos grandes multinacionales, pero también no pocas PYMES, argumentando que el desarrollo del *software* exige considerables inversiones que los terceros no están dispuestos a financiar en ausencia de patentes.

Todos ellos, así como los organismos nacionales, europeos e internacionales abogan por promover el sistema de patentes en este ámbito alegando que las patentes no solo no frenan la innovación, sino que la promueven de dos formas. En primer lugar, permiten que los innovadores recuperen su inversión en actividades de I+D. Si una invención satisface los estrictos criterios de patentabilidad, al solicitante se le recompensa con un derecho exclusivo temporal que impide que terceros (competidores incluidos) hagan uso de la invención patentada sin su consentimiento, a cambio de la divulgación de la invención. Los investigadores innovan sabiendo que posiblemente podrán obtener protección para sus ideas inventivas. Se aduce que, hoy en día, es difícil imaginar que una empresa se plantee lanzar sus productos al mercado sin disponer de una adecuada protección garantizada por patente, sobre todo cuando están en juego costes de desarrollo y niveles de inversión de puesta en marcha elevados, como es el caso. Por consiguiente, una patente suele ser un elemento vital para el éxito de la comercialización. Se trata de un incentivo esencial para innovar y son incontables las innovaciones importantes que han llegado al mercado gracias al sistema de patentes.

Al respecto de las PYMES se observa que la normativa sobre patentes no distingue entre particulares, PYMES y grandes corporaciones. Y aunque es cierto que las grandes empresas disponen de más medios financieros para cubrir los costes de solicitud de una patente, para muchas PYMES y nuevas empresas con pocos recursos financieros y una pequeña cuota de mercado, las patentes son a menudo la única oportunidad para defender su posición frente a la competencia de sus rivales y un instrumento para obtener financiación.

En segundo lugar, el hecho de que todas las solicitudes de patente deban publicarse en un estadio inicial del proceso de obtención de patente garantiza que el público tenga acceso a información sobre las últimas innovaciones. La publicación de este inmenso flujo de nuevas ideas contribuye enormemente a la base de conocimientos de la sociedad. Las bases de datos de patentes de la EPO, por ejemplo, son las mayores

del mundo. Con más de 70 millones de documentos, están disponibles al público gratuitamente en Internet. En tanto que fuente principal de información técnica, actúan como un incentivo para que los inventores desarrollen nuevas soluciones además de las ya patentadas.

Se aduce, además, que el sistema de patentes no existe solo para beneficiar a los innovadores. Los avances tecnológicos benefician al conjunto de los ciudadanos, no solo como consumidores, sino también como individuos pertenecientes a una sociedad industrializada. Los desarrollos tecnológicos, facilitados por el sistema de patentes, ayudan a crear empleo e ingresos y, por consiguiente, contribuyen al crecimiento económico.

Siendo relevante este debate desde los puntos de vista enunciados, lo cierto es que, hoy por hoy, carece de trascendencia en el plano jurídico de *lege data.* No existe ningún obstáculo jurídico derivado de la legislación sobre derecho de autor que impida la protección de los programas de ordenador a través del sistema de patentes. Es más, la compatibilidad está expresamente prevista en el artículo 96.3 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (en adelante, LPI) cuando dispone que "cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial". Asimismo el artículo 8 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, dispone que sus disposiciones se entenderán sin perjuicio de cualesquiera otras disposiciones jurídicas tales como las relativas a los derechos de patente.

Tal y como constata la Decisión de la Cámara de Recursos de la EPO T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998 (ECLI:EP:BA:1998:T117397.19980701) tampoco se opone a la patentabilidad el Acuerdo sobre los ADPIC. La Decisión expresa que la Sala es plenamente consciente de que, de conformidad con el artículo 10 (1) del Acuerdo sobre los ADPIC, "los programas informáticos, ya sean de código fuente o objeto, estarán protegidos como obras literarias en virtud del Convenio de Berna (1971)". Sin embargo, estima, con razón, que esta disposición no debilita la conclusión de que los programas informáticos son patentables en virtud del Acuerdo sobre los ADPIC, según se basa en su artículo 27. El hecho de que el artículo 10 sea la única disposición en los ADPIC que menciona expresamente los programas para computadoras y que los derechos de autor son los medios de protección previstos por dicha disposición no dan lugar a ningún conflicto entre los artículos 10 y 27 del Acuerdo sobre los ADPIC. Los derechos de autor y la protección por patentes constituyen dos medios diferentes de protección legal que, sin embargo, también pueden cubrir el mismo tema (por ejemplo, programas para computadoras), ya que cada uno de ellos cumple su propio propósito.

En efecto, no se trata solo de que exista compatibilidad, que existe. Se trata de que ambos sistemas son cumulativos y deben, considerando la mejor estrategia, ser utilizados a la vez. Y ser completados con la legislación sobre secretos empresariales. A este

respecto ha de tenerse en cuenta la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que incorpora la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. Conforme a ella el objeto de la misma es la protección de los secretos empresariales, estimándose que se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

En este contexto debe valorarse en primer lugar que los efectos técnicos que se producen como consecuencia de la ejecución de los programas no están protegidos mediante derechos de autor, por lo que, en relación con este aspecto, se impone reunir los requisitos que determinan la patentabilidad.

Tampoco están protegidos mediante los derechos de autor las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces (art. 96.4 LPI). En el mismo sentido, el Acuerdo de los ADPIC declara que la protección del derecho de autor abarcará las expresiones, pero no las ideas, procedimientos, métodos de operación o conceptos matemáticos en sí (art. 9.2 ADPCIC). La exclusión del algoritmo como obra protegible queda reflejada en el Considerando 11 de la Directiva 2009/24/CE, sobre la protección jurídica de los programas de ordenador, la cual señala que "*en la medida en que la lógica, los algoritmos y los lenguajes de programación abarquen ideas y principios, estos últimos no están protegidos con arreglo a la presente Directiva*". En la misma línea se expresa el artículo 1.2 de dicha Directiva, que señala que "*Las ideas y principios en los que se base cualquiera de los elementos de un programa de ordenador, incluidos los que sirven de fundamento a sus interfaces, no estarán protegidos mediante derechos de autor con arreglo a la presente Directiva*", así como el artículo 96.4 TRLPI. Por tanto, los algoritmos matemáticos en que se basa la AI no están protegidos por los derechos de autor. De otro lado, según se ha expuesto en los apartados anteriores, salvo que se pueda acreditar la existencia de carácter técnico, los algoritmos se consideran un método matemático excluido, por tanto, del concepto de invención conforme a la legislación sobre patentes. De modo que, en este caso, la opción sería valorar la aplicación de protección mediante la Ley de Secretos Empresariales.

Más problemático es decidir en torno a la especificación de los algoritmos mediante el código fuente y el código objeto. La legislación de sobre derechos de autor protege el código fuente y posiblemente también el código objeto. Ahora bien, protege el código fuente en la medida en que haya sido escrito en el mismo lenguaje de programación. Si se utiliza otro lenguaje es jurídicamente otro texto y, por tanto, está excluido de la tutela.

De otro lado, no existe disposición legal alguna en virtud del CPE que obligue a los solicitantes a presentar el código fuente de un programa; la OEP tampoco lo pide. Tampoco examina los códigos ni los publica como anexos a los documentos de solicitud de patente (la solicitud de concesión, la descripción, las reivindicaciones, los dibujos y el resumen). El código fuente no es necesario para la descripción suficiente de una invención implementada en ordenador. A los efectos de examen y publicación, el concepto inventivo debe describirse en la solicitud de manera suficientemente clara y completa como para que un experto sobre la materia pueda ejecutar la invención, para tal fin no se requiere la divulgación del código fuente.

Según expresan las Directrices de examen EPO F II-4.12 Programas de computador, en el caso particular de las invenciones en el campo de las computadoras, no se puede confiar en las listas de programas en lenguajes de programación como la única divulgación de la invención. La descripción, como en otros campos técnicos, debe estar escrita sustancialmente en un lenguaje normal, posiblemente acompañada de diagramas de flujo u otras ayudas para su comprensión, de modo que la invención pueda ser entendida por un experto en la técnica que no se considere un especialista en cualquier lenguaje de programación específico, pero tiene habilidades generales de programación. Se pueden aceptar breves extractos de programas escritos en lenguajes de programación comúnmente usados si sirven para ilustrar una realización de la invención. Por tanto, parece claro que las patentes de *software* no protegen el código fuente.

Como ejemplo se cita la patente de Microsoft concedida en 2004 en EEUU bajo el número 6727830: "*Time based hardware button for application launch*". En este caso, simplemente protege el control de una aplicación mediante un *click* del ratón, en función del tiempo que se ha mantenido pulsado. Dicha patente no reivindica el código fuente como tal empleado para ponerlo en funcionamiento, lo cual dependería del lenguaje de programación empleado y del *hardware* al que va destinado La patente se centra en proteger un método que comprende la detección de la pulsación de un botón de un dispositivo (como el ratón), el cómputo del tiempo de pulsación del mismo y, en función de si dicho tiempo de pulsación supera un determinado umbral, la ejecución de una u otra acción con la aplicación a la que esté asociada el botón. Esta innovación se pudo patentar en EEUU porque consistía en aumentar la funcionalidad de un botón en función de su tiempo de pulsación, pero no pudo ser patentado en Europa. Otra patente famosa es la que se concedió a Amazon en 1999 en EEUU bajo la denominación US5960411, en este caso referida a un método para preparar una orden de compra mediante un único *click* de ratón (función conocida como *one-click*). Igualmente, sólo se concedió en Estados Unidos, mientras que en Europa la patente se revocó al ser los requisitos de patentabilidad para este tipo de invenciones más estrictos.

Por tanto, las patentes tampoco se muestran como una solución completa en relación con la IA. No protegen las compilaciones de datos, como los conjuntos de capacitación en inteligencia artificial, la expresión particular del código fuente de un programador u otro tipo de información patentada que puede ser competitivamente ventajosa y constituir un secreto comercial.

Con todo, no hay que sobrevalorar la permisibilidad de la concesión de patentes en EEUU por encima de lo que ocurre en Europa. El sistema de patentes en EEUU presenta incertidumbres importantes con respecto a la patentabilidad en relación con ciertos aspectos de la IA, como el software. Desde la decisión de la Corte Suprema en el caso Alice v. CLS Bank, en que el tribunal dictaminó que una idea abstracta no se vuelve elegible para una patente simplemente por ser implementada en una computadora genérica, muchas de estas patentes han sido atacadas e invalidadas como patentes inelegibles en aplicación del artículo 35 USC § 101. Bajo este régimen, la decisión de solicitar una patente puede tener graves consecuencias: si se solicita una patente pero no se obtiene, o se otorga y luego se invalida, la materia puede haberse hecho pública, lo que hace que no solo la protección mediante patente, sino también la protección de secretos comerciales no esté disponible.

Bibliografía

AA.VV: *Comentarios a la Ley de Propiedad intelectual* (dir. PALAU RAMÍREZ, F/PALAO MORENO, G, Valencia, Tirant lo Blanch, 2018.

BLANCO, JM/ COHEN, J. "Inteligencia artificial y poder", *ARI* (93) 2018, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari93-2018-blanco…, pags. 1 y ss.

BOTANA AGRA, M: "Invenciones patentables", en *Manual de la Propiedad Industrial,* Madrid, Marcial Pons, 2009, págs.., 107 y ss., 109.

COMISIÓN EUROPEA: Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones -Plan coordinado sobre la inteligencia artificial 7.12.2018, y ANEXO *www.ipex.eu/IPEXL-WEB/dossier/files/.../082dbcc5679fb7b40167a1b3f76300c1.do*

COMISIÓN EUROPEA: Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones- Inteligencia artificial para Europa de 25 de abril de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES

CONSEJO DE LA UNIÓN EUROPEA: Conclusiones relativas al Plan Coordinado sobre el Desarrollo y Uso de la Inteligencia Artificial «Made in Europe», 11 de febrero de 2019, https://www.consilium.europa.eu/es/press/press-releases/2019/02/18/european-coordinated-plan-on-artificial-intelligence/

DE LA CUEVA GONZÁLEZ-COTERA,J: "La importancia del código fuente", en *Derecho digital: retos y cuestiones actuales*, Cizur Menor, 2018, consultado en Proview

Decisión de la Cámara de Recursos EPO T 1173/97 (producto de programa de computadora / IBM) de 1.7.1998, ECLI:EP:BA:1998:T117397.19980701.

Decisión de la Cámara de Recursos EPO T 0258/03 (Método de subasta / HITACHI) de 21.4.2004, ECLI: EP: BA: 2004: T025803.2004042.

Decisión de la Sala de Recursos EPO T 424/03 (formatos de Portapapeles I / MICROSOFT) de 23.2.2006, ECLI: EP: BA: 2006: T042403.20060223

Decisión de la Cámara de Recursos EPO T 1227/05 (Simulación de circuito I / Infineon Technologies) de 13.12.2006, ECLI: EP: BA: 2006: T122705.20061213

Decisión de la Alta Cámara de Recurso G 0003/08 (Programas para ordenadores) del 12.5.2010, ECLI: EP: BA: 2010: G000308.20100512)

Decisión de la Sala de Recursos EPO T 1784/06 (Método de clasificación / COMPTEL) de 21.9.2012, ECLI: EP: BA: 2012: T178406.20120921

Decisión de la Sala de Recursos EPO T 1316/09 () de 18.12.2012, ECLI: EP: BA: 2012: T131609.20121218

Decisión de la Sala de Recursos EPO T 1358/09 (Clasificación / BDGB SOFTWARE EMPRESARIAL) de 21.11.2014, ECLI: EP: BA: 2014: T135809.20141121

Decisión de la Sala de Recursos EPO T 1370/11 (Sistema de propiedad a demanda / MICROSOFT) del 11.3.2016, ECLI: EP: BA: 2016: T137011.20160311

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

Directrices de examen de solicitudes de patente elaboradas por la Oficina española de Patentes y Marcas, https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Invenciones/DirExPat_DIRECTRICES_Version_2_0.pdf

EPO-Guidelines2018- disponible en https://www.epo.org/law-practice/legal-texts/html/guidelines2018

FERNÁNDEZ MASIÁ., E: "Programas de ordenador", en AA.VV: *Comentarios a la Ley de Propiedad intelectual* (dir. PALAU RAMÍREZ, F/PALAO MORENO, G, Valencia, Tirant lo Blanch, 2018, versión e-book, págs.. 1183 y ss.

HOFFMAN-RIEM, W: *Big Data. Desafíos también para el Derecho,* Cizur Menor, Aranzadi, 2018.

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

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

NAVAS NAVARRO, S. <<Derecho e inteligencia artificial desde el diseño. Aproximaciones>>, en AA. VV. *Inteligencia artificial,* Valencia, Tirant lo Blanch, *2017, págs. 23 y ss.,* 24 y 25.

RODRÍGUEZ GARCÍA, J.A/ MORENO REBATO, M.: "¡El futuro ya está aquí! Derecho e Inteligencia artificial", Revista Aranzadi de Derecho y Nuevas Tecnologías 48 (2018), consultado en Proview, págs.. 1 y ss

Reglamento de ejecución del Convenio sobre la patente europea, adoptado por Decisión del Consejo de Administración de la Organización Europea de Patentes de 12 de diciembre de 2002 y modificado por última vez por Decisión del Consejo de Administración de la Organización Europea de Patentes de 14 de diciembre de 2016.

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

THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN – USA 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf.

TUTT, A: "An FDA for algorithms", *Administrative Law Review* 83 (2017), ttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994, págs.. 1 y ss

VI V I 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), https://ieeexplore.ieee.org/document/8114708, págs, 2295 y ss

Proyecto: *Análisis y seguimiento de los derechos digitales y ética digital*

Actividad 2: Avance del proyecto de elaboración de la *Carta de derechos digitales de la provincia de Alicante*

JUSTIFICACIÓN

El objetivo prioritario del proyecto es acometer la tarea de reconocer un espectro amplio de derechos digitales que permitan garantizar los derechos y libertades de la ciudadanía sumando a la protección jurídica de que disponemos aquella otra que resulta necesaria el entorno digital.

En este sentido, gracias a la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales que contempla el derecho al olvido en la red, la seguridad y la educación digital o la desconexión digital en el ámbito laboral, se dio un primer paso para garantizar algunos derechos digitales.

En una sociedad y economía cada vez más digitalizadas, es fundamental enfrentarse a cuestiones como el derecho a la privacidad y la seguridad, la protección frente a la violencia, la educación, la reducción de las brechas digitales, así como sus dimensiones laborales y civiles. En particular, se debe prestar especial atención a asegurar que la digitalización no deje desprotegidos a los más vulnerables.

Entendemos que corresponde a los poderes públicos impulsar políticas que hagan efectivos tales derechos promoviendo la igualdad de los individuos y de los grupos en los que se integra para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital.

Por todo ello, pretendemos elaborar una Carta de derechos digitales de la provincia de Alicante que recogerá los derechos susceptibles de protección digital del conjunto de la ciudadanía alicantina y nos permitirá colocarnos a la vanguardia nacional en relación con el desarrollo de una sociedad digital libre, abierta e inclusiva.

Con el fin de contar con la mayor participación de la sociedad civil alicantina, oportunamente se propondrá una consulta pública para recabar su opinión ya sea a título individual o a través de asociaciones representativas de la provincia de Alicante.

En la elaboración de esta Carta ha de garantizarse, por una parte, el respeto a los derechos humanos esenciales y los principios democráticos de la sociedad, teniendo en cuenta que el avance tecnológico imparable en que está inmersa la sociedad y el uso extendido de las TIC por parte de la ciudadanía han puesto de manifiesto nuevos peligros para las personas que hay que preservar, especialmente en ámbitos tan esenciales como el derecho a la intimidad, la privacidad o el derecho al honor. Y por otra, asegurar que la persona y sus derechos esenciales sean el centro sobre el que gravite la evolución de las tecnologías y las consecuencias jurídicas derivadas de ello.

El resultado de este trabajo será la Carta de derechos digitales que hará énfasis en derechos tales como el derecho a la identidad digital; derecho de la ciudadanía digital; derecho a la intimidad y confidencialidad en el entorno digital; derecho al olvido y al recuerdo digital; derecho a la protección de los datos personales; derecho a la libertad de pensamiento, expresión e información en el entorno digital; derecho a la educación y formación digital; derecho a la libertad de empresa y desarrollo tecnológicos; derecho a la igualdad y prohibición de discriminaciones ante el uso de las tecnologías; derecho de asilo; derecho a la protección de los menores, personas con diversidad funcional y otros colectivos vulnerables; derecho a la protección de las personas trabajadoras en entornos tecnológicos; derecho a la protección de las personas consumidoras y usuarias en entornos digitales y derecho a la tutela efectiva en los conflictos digitales, entre otros.

Ahora bien, la posición del Derecho – entendido aquí no tanto como ciencia o técnica, sino como el medio a través del cual se expresa la voluntad de lo que una comunidad considera que deben ser los criterios conforme a los cuales se organiza – debe ser la de favorecer, incentivar y sacar provecho de las tecnologías, instrumentos, programas y dispositivos que conforman el universo de la sociedad digital.

Por tanto, hay que evitar impedir o limitar su empleo, si no existe riesgo alguno para los derechos fundamentales y libertades que, de acuerdo con el artículo 10 de nuestra Constitución, son el fundamento del orden político y de la paz social. Ahora bien, precisamente porque se quiere potenciar el empleo y difusión de la sociedad digital –y en la medida que determinados usos de la misma pueden poner en peligro derechos, principios y valores fundamentales recogidos en nuestra Constitución – ello exige una regulación por el Derecho que, a la vez que garantiza el desarrollo y empleo de las técnicas e instrumentos propios de la sociedad digital, proteja dichos valores, principios y derechos.

En este sentido cabe subrayar que una regulación muy detallada, precisa e intervencionista en los momentos emergentes de la sociedad digital –y de sus técnicas e instrumentos – puede ser negativa en cuanto asfixie las posibilidades de desarrollo cuando todavía no se conocen bien todas sus posibilidades y efectos.

Finalmente, deberíamos plantearnos si es conveniente establecer algún organismo regulador para el desarrollo y funcionamiento de la sociedad digital, pues no siempre el legislador –ni el plano normativo– está en las mejores condiciones para culminar la regulación, por las peculiaridades técnicas que ofrece cada uno de los campos en que incide la sociedad digital y su constante evolución y progreso.

STATUS QUAESTIONIS

Recientemente, la Secretaria de Estado de Digitalización e Inteligencia Artificial ha hecho pública la Carta de derechos digitales fruto del trabajo realizado por un grupo de expertos que ha de ser tomada en consideración, al menos inicialmente y con la debida cautela dado su carácter provisional, como marco jurídico para el desarrollo de la Carta que se elaborará a nivel provincial. En todo caso, se advierten algunas contradicciones en el texto que será necesario corregir e instaremos a ello en el momento oportuno.

Igualmente, existen otras iniciativas propiciadas por el Colegio de Abogados de Barcelona o por el propio Ayuntamiento de la Ciudad Condal que han ultimado Cartas de derechos digitales de ámbito local que también serán sometidas a examen. El elenco de derechos relacionados es el siguiente:

Derecho a la identidad digital
Derecho a la ciudadanía digital
Derecho a la dignidad y al libre desarrollo de la personalidad ante los desarrollos tecnológicos
Derecho a la libertad e igualdad en el acceso al entorno digital
Derecho a la seguridad ante los desarrollos tecnológicos
Derecho a la intimidad y confidencialidad en el entorno digital
Derecho al olvido y al recuerdo digital
Derecho a la protección de los datos personales
Derecho a la libertad de pensamiento, expresión e información.
Derecho a la educación y formación profesional digital
Derecho a la libertad de empresa y desarrollos tecnológicos
Derecho a la propiedad intelectual en entornos tecnológicos
Derecho a la igualdad y prohibición de discriminación ante el uso de las nuevas tecnologías
Derecho a la protección de los menores, personas con diversidad funcional y otros colectivos vulnerables
Derecho a la protección de las personas trabajadoras en entornos tecnológicos
Derecho al desarrollo tecnológico sostenible

Derecho a la protección de las personas consumidoras y usuarias en entornos digitales
Derecho al asilo digital
Derecho a la participación en asuntos públicos y
Derecho a la tutela efectiva en los conflictos digitales

Por consiguiente, con las cautelas antedichas, entendemos imprescindible tomar como punto de referencia la Carta de derechos digitales sometida a exposición pública por el Ministerio de Asuntos Económicos y Transformación Digital y proceder a su análisis detallado, así como al estudio de todos aquellos trabajos presentados sobre la materia. No obstante, la Carta de derechos digitales de la provincia de Alicante no será un mero compendio de los derechos ya reconocidos sino que realizará aportaciones jurídicas novedosas debidamente fundamentadas que la doten de singularidad.

ANEXO I

CARTA DE DERECHOS DIGITALES

DERECHOS DE LIBERTAD

I.- Derechos y libertades en el entorno digital

1. Los derechos fundamentales y libertades reconocidos en nuestra Constitución, en la Declaración Universal de Derechos Humanos, la Carta de los Derechos Fundamentales de la Unión Europea y en los tratados y acuerdos internacionales sobre las mismas materias ratificados por España están garantizados en el entorno o espacio1 digital.

1 A los efectos de esta Carta, por entorno digital se entiende el conjunto de sistemas, aparatos, dispositivos, plataformas e infraestructuras que abren espacios de relación, comunicación, interrelación, comercio, negociación, entretenimiento y creación que permiten a las personas físicas o jurídicas de forma bilateral o multilateral establecer relaciones semejantes a los existentes en el mundo físico tradicional. Espacio digital se refiere a los lugares digitales que abren los entornos digitales en los que es posible la comunicación, interrelación, comercio, negociación, entretenimiento y creación de forma especular con el mundo físico tradicional. La ciudadanía digital se refiere al estatuto de derechos y obligaciones de la persona, con independencia de su estatuto jurídico de nacional.

2. Todas las personas poseen idénticos derechos en el entorno digital y en el analógico, sin perjuicio de las limitaciones que de acuerdo con la Constitución y las leyes pudieran establecerse atendiendo a las peculiaridades de cada ámbito.

3. Las leyes concretarán, en cuanto sea necesario, las especificidades de los derechos en el entorno digital y regularán su desenvolvimiento y efectividad estableciendo garantías y promoviendo la igualdad en el ecosistema digital.

4. Los procesos de transformación digital, el desarrollo y el uso de la tecnología digital, así como cualquier proceso de investigación científica y técnica relacionado con ellos o que los utilice instrumentalmente, deberán tener presente la exigencia de garantizar la dignidad humana, los derechos fundamentales, el libre desarrollo de la personalidad y ordenarse al logro del bien común.

5. El principio de cumplimiento normativo desde el diseño deberá aplicarse íntegramente al desarrollo científico y tecnológico, así como a sus resultados. Los desarrollos científicos y tecnológicos contemplarán en la determinación de sus requerimientos un análisis sobre el cumplimiento de tal principio.

II.- Derecho a la protección de datos

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

III.- Derecho a la identidad en el entorno digital

1. Se reconoce el derecho a la propia identidad en el entorno digital, de acuerdo con el ordenamiento jurídico nacional y europeo.
2. La identidad no podrá ser alterada, controlada o manipulada por terceros contra la voluntad de la persona.
3. Se establecerán las garantías que permitan preservar y controlar la propia identidad en el entorno digital.

IV.- Derecho al pseudonimato

1. De acuerdo con las posibilidades técnicas disponibles los entornos digitales permitirán el acceso en condiciones de pseudonimidad.
2. El diseño de la pseudonimidad a la que se refiere el párrafo anterior asegurará la posibilidad de reidentificar a las personas en los casos y con las garantías previstos por el ordenamiento jurídico.

V.- Derecho a no ser localizado y perfilado

1. El derecho a la libre autodeterminación individual y la garantía de las libertades comporta el derecho a no ser objeto de localización, ni a ser sometido a análisis de la personalidad o conducta que impliquen el perfilado de la persona.
2. Sólo serán posibles tales tratamientos de información personal con el consentimiento de la persona afectada o en los casos y con las garantías previstos en las leyes.

VI.- Derecho a la seguridad digital

1. Toda persona tiene derecho a la seguridad en el entorno digital.
2. Los poderes públicos adoptarán y promoverán las medidas necesarias para garantizar aquélla, en colaboración siempre con las empresas tecnológicas y con los usuarios.

VII.- Derecho a la herencia digital

1. Se reconoce el derecho a la herencia digital de todos los bienes y derechos de los que sea titular la persona fallecida en el entorno digital.
2. El acceso a contenidos y servicios digitales de los que fuera titular la persona fallecida se hará conforme a las reglas generales del Código Civil, las leyes de las Comunidades autónomas con derecho civil, foral o especial, propio y el Título X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

DERECHOS DE IGUALDAD

VIII.- Derecho a la igualdad y a la no discriminación en el entorno digital

1. Se reconoce el derecho a la igualdad en los entornos digitales, la no discriminación y la no exclusión. En particular, se reconoce el derecho a la igualdad efectiva de mujeres y hombres en entornos digitales. Los procesos de transformación digital aplicarán la perspectiva de género.

2. Los poderes públicos impulsarán políticas ordenadas a la garantía del acceso efectivo de todas las personas a los servicios y oportunidades que ofrecen los entornos digitales en cualquiera de sus dimensiones, garantizarán el derecho a la no exclusión digital y combatirán las brechas digitales en todas sus manifestaciones, atendiendo particularmente a la brecha territorial y asegurando un derecho de acceso universal, asequible, de calidad y no discriminatorio a Internet para toda la población.

IX.- Protección de menores en el entorno digital

1. Los progenitores, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos, de los entornos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en entornos digitales en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

3. Salvo en las excepciones previstas en las leyes, se prohíben los tratamientos de la información de los menores orientados a establecer perfiles de personalidad en entornos digitales.

4. Se consideran ilícitas las prácticas de perfilado susceptibles de manipular o perturbar la voluntad de los menores y, en particular, la publicidad basada en este tipo de técnicas.

5. Se impulsará el estudio del impacto en el desarrollo de la personalidad de los menores derivado del acceso a entornos digitales, así como a contenidos nocivos o peligrosos. Dicho estudio prestará particular atención a sus efectos en la educación afectivo-sexual, las conductas dependientes, la igualdad de género, así como los comportamientos antidemocráticos, racistas y violentos.

X.- Protección de personas con discapacidad en el entorno digital

1. Se garantizará la accesibilidad de los entornos digitales a las personas con discapacidad tanto desde el punto de vista tecnológico como respecto de sus contenidos. En particular, asegurarán que la información relativa a las condiciones legales del servicio resulte accesible y comprensible.

2. Los entornos digitales, y en particular los que tengan por finalidad la participación política digital, asegurarán la participación efectiva de las personas con discapacidad o diversidad funcional.

3. Se garantizará el derecho a la educación digital de las personas con discapacidad.

XI.- Protección de las personas mayores en el entorno digital

1. Se reconoce el derecho de las personas mayores al acceso a los entornos digitales.
2. Se garantizará la accesibilidad a los entornos digitales a las personas de este colectivo.

DERECHOS DE PARTICIPACIÓN Y DE CONFORMACIÓN DEL ESPACIO PÚBLICO

XII.- Derecho a la neutralidad de Internet

Los poderes públicos garantizarán el derecho de los usuarios a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos, en los términos previstos en el Reglamento (UE) 2015/2120 de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

XIII.- Libertad de Expresión y Libertad de Información

1. Todos tienen derecho a las libertades de expresión e información en entornos digitales en los términos previstos por la Constitución. Se garantizarán los principios constitucionales relativos a la veracidad, el pluralismo informativo y la diversidad de opiniones e informaciones.
2. Los responsables de medios de comunicación, así como los de los entornos digitales que o bien tengan por objeto el ejercicio de libertades del párrafo anterior por sus titulares o bien provean tal servicio a sus usuarios, adoptarán protocolos adecuados para garantizar los derechos de todas las personas a:
a) Conocer cuándo la información sea elaborada sin intervención humana mediante procesos automatizados.
b) A conocer cuándo una información ha sido clasificada o priorizada por el proveedor mediante técnicas de perfilado o equivalentes. Cuando esta información sea patrocinada por un tercero deberá informarse de modo específico sobre la naturaleza publicitaria de la misma.
c) A solicitar del prestador la no aplicación de técnicas de análisis que permitan ofrecer información que afecte a las libertades ideológica, religiosa, de pensamiento o creencias.
d) A posibilitar el ejercicio del derecho rectificación ya sea frente a medios de comunicación, ya sea ante aquellos usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación. Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación

en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.
e) A solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.
En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.
3. Los procesos de verificación y retirada de contenidos se limitarán a aquellos que en entornos digitales se encuentran limitados por la prohibición de censura previa. En los supuestos en los que la ley ampare la retirada de un contenido, los prestadores deberán notificarla al usuario y disponer de un procedimiento de reclamación de estas decisiones. Se impulsarán mecanismos de autorregulación transparentes que contemplen los criterios y los procedimientos que determinan en este ámbito la actuación de los prestadores e incorporen procedimientos de reclamación y revisión de las decisiones de retirada de contenidos.

XIV.- Derecho a la participación ciudadana por medios digitales

1. De acuerdo con las leyes, se impulsarán procedimientos de participación de las personas en la vida pública.
Para ello, se promoverán entornos digitales que contribuyan a un derecho de acceso efectivo a la información pública, la transparencia, la rendición de cuentas, así como a la propuesta, e implicación de las personas en las actuaciones de las Administraciones públicas en sus respectivos ámbitos competenciales, de acuerdo con la Constitución.
2. Los procedimientos de participación ciudadana garantizarán condiciones de igualdad sin discriminaciones ni exclusión de personas, con sujeción al ordenamiento jurídico.

XV.- Derecho a la educación digital

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.
2. El profesorado recibirá la formación para adquirir las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.
3. En particular los poderes públicos con competencia en la materia promoverán:
a) Los planes de formación profesional que se ordenarán a la inserción de las personas trabajadoras en los procesos de transformación digital.
c) La formación de personas adultas con particular atención a los mayores.
d) La educación audiovisual en el entorno digital, con la finalidad de promover la capacidad crítica y afrontar las prácticas de desinformación.

4. Se reconoce el derecho a la libertad de acceso a la educación y a la libertad de creación de centros que presten sus servicios a través de entornos digitales, sin perjuicio de lo dispuesto en las leyes respecto al cumplimiento de la normativa educativa y de la obligación de la escolarización presencial en los niveles de educación obligatoria.
5. Se impulsará la Educación para la Ciudadanía Digital, porque una parte esencial de la estrategia de digitalización de la educación pasa por el desarrollo de competencias que permitan que el uso de las tecnologías sea beneficioso para cada individuo y para el conjunto de la sociedad. Esta dimensión pasa por cuestiones como:
a) Que los estudiantes aprendan a hacer un uso ético de las herramientas digitales en cuestiones como el uso de datos y el respecto a la privacidad ajena; o la identificación de información y comportamientos en la red que puede comprometer su salud o bienestar y la de terceros.
b) Fortalecer el desarrollo del pensamiento crítico que les ayude a distinguir hechos objetivos de meras opiniones sin evidencias, que les permitan rechazar estereotipos discriminadores, los discursos de odio o el ciber acoso.
c) Fomentar también la capacidad de participar en la generación de información de manera activa, creativa y, sobre todo, responsable.
d) Atender la diversidad de talentos y de procesos y ritmos de aprendizaje, particularmente aquéllos que tienen necesidades específicas de apoyo educativo.

XVI.- Derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas

1. Se reconoce el derecho de igualdad en el acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas. A tal fin se promoverán políticas públicas activas que garanticen el acceso a los sistemas y los procedimientos.
2. El poder público autor de una actividad en el entorno digital deberá identificar a los órganos responsables de la misma.
3. El principio de transparencia y de reutilización de datos de las Administraciones públicas guiará la actuación de la Administración digital, de conformidad con la normativa sectorial. En particular, se garantizará el derecho de acceso a la información pública, se promoverá la publicidad activa y la rendición de cuentas y se velará por la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones.
4. Siempre que sea posible se promoverá la universalidad y la neutralidad de las tecnologías usadas por las Administraciones públicas, así como su diseño y uso conforme a los principios éticos que acompañan a esta Carta. Así mismo se adoptarán las medidas precisas para garantizar que la prestación de los proveedores de servicios que colaboren con ellos por medios digitales se realicen conforme a las disposiciones de esta Carta.
5. Se ofrecerán alternativas en el mundo físico que garanticen los derechos de aquellas personas que opten por no utilizar recursos digitales.
6. Los daños causados por actividades o decisiones digitales, podrán dar lugar a un derecho a la indemnización por toda lesión que las personas físicas o jurídicas sufran en cualquiera de sus bienes y derechos, de acuerdo con las leyes
7. Los derechos de la ciudadanía en relación con la Inteligencia Artificial reconocidos en esta Carta resultarán también de aplicación en el marco de la actuación

administrativa, en particular en los aspectos referidos al diseño y al uso de algoritmos. En todo caso, se reconoce el derecho a:
a) Que las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital.
b) Un procedimiento de toma de decisiones con las debidas garantías.
c) Obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes al caso y de los criterios de aplicación de las mismas
d) Que la adopción de decisiones discrecionales quede reservada a personas, salvo que una norma con rango de ley permita la adopción de decisiones automatizadas en este ámbito.
Será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas. En todo caso, serán objeto de aprobación previa de los sistemas algorítmicos que se vayan a usar para la toma de decisiones, con determinación de su ámbito concreto de aplicación y estructura de funcionamiento.

DERECHOS DEL ENTORNO LABORAL Y EMPRESARIAL

XVII.-Derechos en el ámbito laboral

1. En el ámbito laboral trabajadores y los empleados públicos tienen derecho a:
a) La desconexión digital.
b) La protección de su intimidad en el uso de dispositivos digitales puestos a su disposición por su empleador, así como frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
c) La intimidad ante la utilización de sistemas de geolocalización.
En todo caso se garantizarán condiciones de trabajo digno en los entornos digitales.
2. Cuando la naturaleza del puesto y las capacidades de la organización lo permitan se promoverán condiciones de acceso al teletrabajo. En este caso, la ordenación de la prestación laboral se desarrollará con pleno respeto a la dignidad de la persona trabajadora garantizando particularmente su derecho a la intimidad, la esfera privada del domicilio, los derechos de las personas que residen en él y el derecho a la conciliación de la vida personal y familiar.
3. En los procesos de transformación digital:
a) Deberá proporcionarse a las personas trabajadoras una formación adecuada que permita su adaptación a las nuevas condiciones laborales;
b) Se informará a la representación de los trabajadores sobre los cambios tecnológicos que vayan a producirse en la empresa y a participar en la toma de decisiones sobre la transformación digital y las consecuencias laborales que la misma pueda implicar;
4. Sin perjuicio del derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, salvo en los supuestos previstos por la ley, se informará a los representantes de los trabajadores y las personas directamente afectadas sobre el uso de la analítica de datos o sistemas de inteligencia artificial en la gestión, monitorización y procesos de toma de decisión en materia de recursos humanos y relaciones laborales. Este deber de información alcanzará como mínimo al

conocimiento de los datos que se utilizan para alimentar los algoritmos, su lógica de funcionamiento y a la evaluación de los resultados.

XVIII.- La empresa en el entorno digital

1. Se reconoce la libertad de empresa en los entornos digitales en el marco de la economía de mercado. El desarrollo tecnológico y la transformación digital de las empresas deberán respetar los derechos digitales de las personas.
2. Los poderes públicos promoverán la investigación, el desarrollo tecnológico y la innovación ordenados a la transformación digital de las empresas, el emprendimiento digital y el fomento de las capacidades de la sociedad para la generación de ciencia y tecnología nacionales.
3. Se desarrollarán las condiciones que permitan la creación de espacios de pruebas controladas para desarrollar nuevos modelos de negocio, aplicaciones, procesos o productos basados en la tecnología (sandbox).

DERECHOS DIGITALES EN ENTORNOS ESPECÍFICOS

XIX.- Derecho de acceso a datos con fines de investigación científica, innovación y desarrollo

1. El uso de los datos del sector público y privado para el bien común se considera un bien de interés general.
2. En el marco definido por las leyes se promoverán condiciones que garanticen la reutilización de la información y el uso de los datos para promover la investigación, la innovación y el desarrollo.
3. Cuando se trate de datos personales:
a) Los datos podrán ser tratados con fines de investigación científica, innovación y desarrollo previa anonimización.
b) Únicamente será admisible el tratamiento de datos personales o pseudonimizados cuando la naturaleza de la actividad lo requiera y se cuente con el consentimiento o una autorización expresa prevista en norma con rango de ley.
c) Se promoverán programas de donantes de datos para fines de investigación.
En todo caso serán de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y la legislación sectorial que corresponda.
4. El desarrollo de la investigación científica y tecnológica susceptible de repercutir en el ser humano respetará su dignidad y garantizará a toda persona, sin discriminación alguna, el respeto a su integridad y a sus demás derechos y libertades fundamentales con respecto a las aplicaciones de la biología y la medicina.
5. La investigación en áreas como la neurociencia, la genómica o la biónica, entre otras, aplicará lo dispuesto en los párrafos anteriores y, en particular, garantizará el

respeto a la dignidad, la libre autodeterminación individual, la intimidad y la integridad de las personas.

XX.- Derecho a un desarrollo tecnológico y a un entorno digital sostenible

1. El desarrollo de la tecnología y de los entornos digitales deberá perseguir la sostenibilidad medioambiental y el compromiso con las generaciones futuras.
2. Los poderes públicos impulsarán políticas ordenadas a la consecución de tales objetivos con particular atención a la sostenibilidad, durabilidad, reparabilidad y retrocompatibilidad de los dispositivos y sistemas evitando las políticas de sustitución integral y de obsolescencia programada.
3. Los poderes públicos promoverán la eficiencia energética en el entorno digital, favoreciendo la minimización del consumo de energía y la utilización de energías renovables y limpias.

XXI.- Derecho a la protección de la salud en el entorno digital

1. Se reconoce el derecho de todas las personas al acceso a los servicios digitales de salud en condiciones de igualdad, accesibilidad y universalidad.
2. Los poderes públicos promoverán que la investigación y la tecnología contribuyan al logro de una medicina preventiva, predictiva, personalizada, participativa y poblacional.
2. El sistema de salud garantizará el desarrollo de sistemas de información que aseguren la estandarización, la interoperabilidad, el acceso y la portabilidad de la información del paciente.
3. El empleo de sistemas digitales de asistencia al diagnóstico, y en particular de procesos basados en inteligencia artificial no limitará el derecho a la libertad diagnóstica del personal facultativo.
4. Los entornos digitales de salud garantizarán el pleno respeto de los derechos fundamentales del paciente y en particular su derecho a ser informado y consentir en el tratamiento de sus datos personales con fines de investigación y en la cesión a terceros de tales datos cuando tal consentimiento sea requerido.
6. Los poderes públicos impulsarán el acceso universal de la población a los dispositivos tecnológicos desarrollados con fines terapéuticos o asistenciales.

XXII.- Libertad de creación y derecho de acceso a la cultura en el entorno digital

1. Se reconoce el derecho a la libertad de creación en el entorno digital, promoviendo programas de formación en el sistema educativo y garantizando el derecho a la remuneración del personal creativo.
2. Se garantizará el acceso a la cultura en el entorno digital, en los términos de los artículos 44.1 y 149.2 de la Constitución Española, así como de la Convención de la UNESCO sobre la protección y la promoción de la diversidad de las expresiones culturales, de 20 de octubre de 2005. En todo caso se tendrán en cuenta las normas sobre propiedad intelectual y los derechos derivados.
3. En particular, los poderes públicos facilitarán el acceso digital a las diversas manifestaciones artísticas y culturales en espacios de su titularidad o de terceros con

quienes colaboren de forma directa o indirecta. En particular, se promoverá el acceso digital a obras de dominio público.

XXIII.- Derechos ante la Inteligencia artificial

1. En el desarrollo y ciclo de vida de los sistemas de Inteligencia Artificial:
a) Se deberá garantizar el derecho a la no discriminación algorítmica, cualquiera que fuera su origen, causa o naturaleza del sesgo, en relación con las decisiones y procesos basados en algoritmos.
b) Se asegurarán la transparencia, auditabilidad, explicabilidad y trazabilidad.
c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.
2. Las personas tienen derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, incluidas aquéllas que empleen procedimientos de inteligencia artificial, que produzcan efectos jurídicos o les afecten significativamente de modo similar, salvo en los supuestos previstos en las leyes. En tales casos se reconocen los derechos a:
a) Solicitar una supervisión e intervención humana;
b) Impugnar las decisiones automatizadas o algorítmicas.
3. Se deberá informar a las personas sobre el uso de sistemas de Inteligencia Artificial que se comuniquen con seres humanos utilizando el lenguaje natural en todas sus formas. Deberá garantizarse en todo caso la asistencia por un ser humano a solicitud de la persona interesada.
4. Se prohíbe el uso de sistemas de Inteligencia Artificial dirigidos a manipular o perturbar la voluntad de las personas, en cualesquiera aspectos que afecten a los derechos fundamentales.

XXIV.- Derechos digitales en el empleo de las neurotecnologías

1. Las condiciones, límites y garantías de implantación y empleo en las personas de las neurotecnologías serán reguladas por la ley con la finalidad de:
a. Preservar la identidad individual como conciencia de la persona sobre sí misma.
b. Garantizar la autodeterminación individual, soberanía y libertad en la toma de decisiones.
c. Asegurar la confidencialidad y seguridad de los datos obtenidos o relativos a sus procesos cerebrales y el pleno dominio y disposición sobre los mismos.
d. Ordenar el uso de interfaces persona-máquina susceptibles de afectar a la integridad física o psíquica.
e. Asegurar que las decisiones y procesos basados en neurotecnologías no sean condicionadas por el suministro de datos, programas o informaciones incompletos, no deseados, desconocidos o sesgados, o por intromisión en conexiones neuronales.
2. Para garantizar la dignidad de la persona, la igualdad y la no discriminación, y de acuerdo en su caso con los tratados y convenios internacionales, la ley regulará aquellos supuestos y condiciones de empleo de las neurotecnologías que, más allá de su aplicación terapéutica, pretendan el aumento cognitivo o la estimulación o potenciación de las capacidades de las personas.

XXV.- Garantía de los derechos en los entornos digitales

1. Sin perjuicio de lo dispuesto en la legislación sectorial específica, todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales.
2. Cuando la lesión de tales derechos, o el daño causado, produzca sus efectos en territorio español podrá invocarse la garantía de estos derechos por la autoridad administrativa o el órgano jurisdiccional competente en España.
3. Se promoverán mecanismos de autorregulación regulada y procedimientos de resolución alternativa de conflictos.
4. Los poderes públicos evaluarán las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y propondrán en su caso la realización de reformas oportunas en garantía de los derechos digitales.

LA PROTECCIÓN PENAL DE LA INTIMIDAD Y LOS DATOS PERSONALES FRENTE A LA UTILIZACION ILÍCITA DE MEDIOS DIGITALES

Carmen Juanatey Dorado
Catedrática de Derecho Penal
Universidad de Alicante

I. Introducción

El uso de la tecnología digital ha supuesto un cambio profundo en el desarrollo de la vida de las personas y en sus relaciones sociales. Y, naturalmente, esto ha tenido su reflejo en el Derecho Penal. Muchos delitos presentes ya en los códigos del siglo diecinueve (como el robo o la estafa, por ejemplo) pueden cometerse hoy a través de medios digitales, lo que ha obligado al legislador a ir introduciendo cambios en la descripción de las conductas constitutivas de ilícitos penales; pero, a un mismo tiempo, la transformación digital ha generado la creación de nuevos delitos que describen conductas impensables hace cincuenta años

Aunque son muchos los intereses protegidos por el Derecho penal que pueden verse afectados por el uso de los medios digitales, entre todos estos intereses ocupan un lugar destacado la intimidad y los datos personales. El desarrollo de la tecnología digital ha supuesto grandes ventajas, pero también una elevación del grado de vulnerabilidad de estos derechos individuales ante los posibles usos ilícitos de esta tecnología. Precisamente, tanto el Tribunal Europeo de Derechos Humanos como el Tribunal Constitucional español han coincidido en señalar la necesidad de reforzar la protección de la vida privada para hacer frente a los riesgos derivados de un uso invasivo de las nuevas tecnologías de la comunicación, que, entre otras cosas, facilitan la captación sistemática de imágenes sin que la persona afectada pueda percatarse de ello y su posterior difusión a amplios sectores de la población, así como el almacenamiento y reproducción de datos de carácter personal[1].

En esa línea, nuestro ordenamiento jurídico despliega toda una serie de medidas dirigidas a proteger la intimidad y los datos personales frente a ese tipo de conductas. A esa finalidad sirven, en el ámbito civil, la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen (en adelante, LO 1/82); en el

[1] STEDH de 24 de junio de 2004, V.H. contra Alemania; y, por todas, STC 12/2012, de 30 de enero, FJ 6.

ámbito administrativo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LO 3/2018); y en el ámbito penal, los delitos recogidos bajo la rúbrica "Del descubrimiento y revelación de secretos" que, en los últimos años, han sido objeto de diversas reformas dirigidas a adaptar su regulación a las nuevas formas de ataque derivadas de los avances tecnológicos[2].

En este primer trabajo me voy a ocupar del estudio de algunos de los problemas que suscita la protección penal de la intimidad, lo que incluye los datos personales, ante los riesgos del uso de los medios tecnológicos y la digitalización. En concreto, me centraré en el análisis del tratamiento doctrinal y jurisprudencial de las siguientes cuestiones: el uso no consentido de medios tecnológicos de grabación del sonido o de la imagen; la revelación no consentida de imágenes o grabaciones obtenidas con la anuencia de la persona afectada; y el acceso no autorizado a datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos. Pero, antes de entrar en el análisis de estos casos problemáticos, realizaré una breve exposición de la doctrina del Tribunal Constitucional español relativa a la concepción de los derechos a la intimidad, a la propia imagen, al secreto de las comunicaciones y al control de los datos personales.

II. Delimitación constitucional de los derechos a la intimidad, a la imagen, al secreto de las comunicaciones y a los datos personales

El Tribunal Constitucional, a lo largo de los años ha ido desarrollando a través de numerosas resoluciones una doctrina sobre el distinto ámbito de los derechos a la intimidad, a la propia imagen, al secreto de las comunicaciones y al control de los datos personales,

[2] Bajo el del Título XII "*De los delitos contra la seguridad y libertad*", Capitulo VII "*Del descubrimiento y revelación de secretos*" del Código penal de 1973, se recogían tres preceptos (los arts. 497 a 499) en los que se regulaban las conductas típicas dirigidas a la protección de la intimidad. Así, el artículo 497 establecía: "El que para descubrir los secretos de otro se apoderase de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 5.000 a 100.000 pesetas. Si no los divulgare, las penas serán de arresto mayor y multa de 5.000 a 25.000 pesetas. Esta disposición no es aplicable a los padres, tutores o quienes hagan sus veces en cuanto a los papeles o cartas de sus hijos o menores que se hallen bajo su dependencia". El artículo 498: "El administrador, dependiente o criado que en tal concepto supiere los secretos de su principal y los divulgare será castigado con las penas de arresto mayor y multa de 5.000 a 25.000 pesetas". Y el artículo 499: "El encargado, empleado u obrero de una fábrica u otro establecimiento industrial que en perjuicio del dueño descubriere los secretos de su industria será castigado con las penas de arresto mayor y multa de 5.000 a 50.000 pesetas". La simplicidad de esta regulación contrasta con la actual, notablemente más compleja, como veremos a lo largo de este texto.

interpretación que ha sido asumida —y en parte desarrollada— por el Tribunal Supremo y las audiencias provinciales.

Conforme a esta doctrina, el derecho a la intimidad personal tiene por objeto "garantizar 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"; este derecho —afirma el Tribunal— atribuye a su titular un poder de control sobre la información relativa a su vida privada o, lo que es lo mismo, "el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido". Si bien, el Tribunal ha precisado que la intimidad protegida en el artículo en el artículo 18.1 CE no se reduce necesariamente a la que se desarrolla en un ámbito doméstico o privado[3].

El derecho fundamental a la propia imagen, a juicio del Tribunal, otorga a los individuos la facultad de decidir qué aspectos de su persona desean preservar de la difusión pública: "su ámbito de protección comprende, en esencia, la facultad de poder impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad perseguida por quien la capta o difunde" y, en consecuencia, comprende "la defensa frente a los usos no consentidos de la representación pública de la persona que no encuentren amparo en ningún otro derecho fundamental"[4]. Lo específico de este derecho frente al derecho a la intimidad es la protección frente a las reproducciones de la imagen que, afectando a la esfera personal de su titular, no dan a conocer su vida íntima[5].

En cuanto al secreto de las comunicaciones el Tribunal Constitucional ha afirmado que este derecho consagra, implícitamente, la libertad de las comunicaciones y, de modo expreso, su secreto, al establecer la interdicción de la interceptación o conocimiento antijurídicos de las comunicaciones ajenas. El artículo 18 CE se dirige inequívocamente —afirma el Tribunal— a garantizar la impenetrabilidad de terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma[6].

---

[3] STC 25/2019, de 28 de febrero, F.J. 4º, con referencia a las SSTC 77/2009, de 23 de marzo, F.J. 2º, y 12/2012, de 30 de enero, F.J. 5º, entre otras.

[4] STC 25/2019, de 28 de febrero, F.J. 4º, con referencia a las SSTC 23/2010, de 27 de abril, F.J. 4º y 19/2014, de 10 de febrero, FF. JJ., 4º y 5º

[5] SSTC 156/2001, de 2 de julio, F.J. 3º y 14/2003, de 28 de enero, F.J. 4º, y ATC 28/2004, de 6 de febrero, F.J. 3º.

[6] STC 56/2003, de 24 de marzo, F.J. 2º. En este mismo sentido, SSTC 70/2002, de 3 de abril, F.J. 9º, y 123/2002, de 20 de mayo, F.J. 4º.

Y, por lo que atañe al concepto de secreto, el Tribunal ha afirmado que tiene un carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo personal, lo íntimo o lo reservado[7]. En general, el Tribunal Constitucional establece una clara distinción entre el derecho al secreto de las comunicaciones y el derecho a la intimidad (entendido este último en sentido restrictivo: no todo lo que se dice o hace en un ámbito privado afecta a la esfera de la intimidad —una carta privada puede no contener aspectos íntimos—).

Por último, en lo que respecta al derecho a la protección de los datos personales ha declarado que, "la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así el derecho a controlar el uso de los mismos datos insertos en un programa informático («habeas data») y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[8]. 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"[9], salvo que exista habilitación legal para que los datos puedan ser tratados sin dicho consentimiento"[10]. Su finalidad es impedir el tráfico ilícito y lesivo de esos datos para la dignidad y los derechos del afectado.

Todos estos derechos reconocidos en el artículo 18 de la Constitución —entre los que se encuentra también el derecho al honor—, de acuerdo con el Tribunal Constitucional, a pesar de su estrecha relación en tanto que derechos de la personalidad derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un contenido propio y específico, y su alcance se encuentra delimitado por el de otros derechos y bienes

[7] STC 56/2003, de 24 de marzo, F.J. 2º.
[8] STC 908/2016, de 30 de noviembre, F.J. 3º; con referencia a las SSTC 292/2000, de 30 de noviembre, F.J. 5º; y 94/1998, de 4 de mayo, F.J. 4º)
[9] STC 292/2000, de 30 de noviembre, F.J. 7º
[10] STC 39/2016, de 3 de marzo, F.J. 3º, con referencia a la STC 292/2000, de 30 de noviembre, F.J. 16º.

constitucionales; especialmente, por el ejercicio de las libertades de expresión e información reconocidas en el artículo 20 de la Constitución[11].

De hecho, son precisamente los frecuentes conflictos con estos últimos derechos los que han permitido al Tribunal Constitucional ir fijando criterios para la delimitación de cada uno de ellos, a través del método de la ponderación. Del resultado de la ponderación entre la intimidad, entendida en sentido amplio, y la libertad de expresión e información me ocuparé en las páginas que siguen.

III. Uso no consentido de medios tecnológicos de grabación o reproducción del sonido o de la imagen

1. Regulación penal (art. 197 C.P.)

El Código penal, en su artículo 197.1 sanciona, entre otras conductas, a quien con la finalidad de descubrir los secretos o de vulnerar la intimidad de otro, sin su consentimiento, utilice artificios técnicos de grabación del sonido o de la imagen[12].

Lo que se protege a través de este precepto, y en general a través de los restantes preceptos incluidos bajo el Capítulo I, del Título X del Código penal[13], es la intimidad, lo que comprende los derechos a la propia imagen y al secreto de las comunicaciones. De hecho, el derecho a la propia imagen no es objeto de protección penal específica y autónoma[14], sino que se protege a

---

[11] SSTC 37/89, de 15 de febrero, F.J. 7º; 207/1996, de 16 de diciembre, F.J. 3º; 70/2002, de 3 de abril, F.J. 10º; y 25/2019, de 28 de febrero, F.J. 7º.

[12] El artículo 197.1 dispone: "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

[13] No obstante, con la inclusión en el Código penal del artículo 197 bis, que introdujo el llamado delito de intrusión, un sector de la doctrina y de la jurisprudencia han visto en esta novedad la incorporación, junto a la intimidad, de un nuevo bien jurídico: la seguridad de los sistemas informáticos y de las redes. Sobre esto véase, Doval Pais, A. y Anarte Borrallo, E.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos de descubrimiento y revelación de secretos", en Boix Reig, J.: *Derecho Penal, Parte Especial,* V.I, 2ª ed., Madrid, p. 495.

[14] En esto coincide generalmente la doctrina. Véase, sólo a título de ejemplo, Morales Prats, F., quien considera que la referencia del Código Penal a la propia imagen resulta incluso innecesaria, en Quintero Olivares, G. (Dir.)/Morales Prats, F. (Coord.): *Comentarios a la Parte Especial del Derecho Penal*, 7ª. ed., Cizur Menor, 2008, pág. 404; López Peregrín, C.: *La protección penal del honor de las personas jurídicas*

través del derecho a la intimidad —y también del derecho al honor—; esto es, la utilización de la imagen de una persona, sin su consentimiento, si no lesiona o pone en peligro su intimidad —o su honor— no es objeto de sanción penal. E, igualmente, el secreto de las comunicaciones se protege penalmente en la medida en que la violación de este derecho afecta a la intimidad: la utilización de artificios técnicos de grabación del sonido o de la imagen, si no lesiona o pone en peligro la intimidad no será objeto de la sanción prevista en el artículo 197.1 C.P.

Como hemos visto, el Tribunal Constitucional ha configurado el derecho a la intimidad como un derecho autónomo que otorga a su titular un poder de control sobre la información relativa a la vida privada, sin que dicho control se constriña necesariamente a la información referente al ámbito doméstico o privado. Sin embargo, desde el punto de vista penal y por razones de proporcionalidad y de intervención mínima, en mi opinión, la concreción de la esfera de la intimidad que debe ser protegida a través de los delitos de descubrimiento y revelación de secretos debe desarrollarse en un ámbito más restringido: el interés protegido penalmente ha de afectar a los aspectos más íntimos de la vida privada. Fuera de este ámbito reducido, la protección ha de corresponder a las vías civil y administrativa. Esta idea debe ser la que guíe la interpretación sobre la relevancia penal de los supuestos de utilización no consentida de artificios técnicos de reproducción o grabación del sonido o de la imagen.

Lo anterior obliga a establecer la distinción entre la idea de intimidad en sentido amplio, que haría referencia a ese poder de control sobre cualquier aspecto de la vida privada; y la intimidad en sentido estricto, que comprendería una esfera mucho mas restringida, la que se desarrolla en el ámbito más íntimo y privado de la vida de las personas y que sería el objeto de protección por el Derecho penal (sería un subconjunto dentro del conjunto que representa la intimidad en sentido amplio).

Por tanto, para que entre en acción la vía penal, el artículo 197.1 exige que la grabación o la reproducción de la voz o de la imagen de la persona se realice sin el consentimiento de esta (lo que guarda coherencia con el carácter disponible del derecho a la intimidad); que la conducta se lleve a cabo de forma subrepticia mediante artificios técnicos; y que quien realice la grabación lo haga con la intención de descubrir los secretos de la persona o de vulnerar su intimidad. Pero, a todo ello habría que añadir que esa acción afecte a la esfera más íntima de la vida privada.

Asimismo, el Código penal prevé agravaciones de la conducta en el caso de que se

---

y los colectivos, Valencia, 2000, pág. 47; y Jareño Leal, A.: *Intimidad e imagen: los límites de la protección penal*, Madrid, 2008, págs. 93-96.

difundan, revelen o cedan a terceros los hechos descubiertos o las imágenes grabadas (art. 197.3); cuando la conducta afecte a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere menor de edad o una persona con discapacidad necesitada de especial protección (art. 197.5 C.P.); cuando se persiga un fin lucrativo (art. 197.6 C.P.); cuando se actúe en el seno de una organización o grupo criminal (art. 197 quater C.P.); o en el caso de que el autor sea autoridad o funcionario público que actúe fuera de los casos permitidos por la Ley, sin mediar causa legal por delito y prevaliéndose de su cargo (art. 198 C.P.).

Ahora bien, los problemas han surgido en relación con determinados supuestos en los que resulta controvertido si las grabaciones de la voz o de la imagen pueden constituir una intromisión ilegítima perseguible penalmente, debido a las dificultades a la hora de delimitar el ámbito al que ha de circunscribirse la protección penal de la intimidad y de valorar el carácter consentido o no de la grabación. Aquí habría que distinguir los dos siguientes supuestos que paso a analizar por separado.

2. Grabación de conversaciones o de imágenes por una tercera persona sin el consentimiento de quienes participan en la conversación o en la escena grabadas.

En principio, estas conductas podrían ser constitutivas de un delito de descubrimiento y revelación de secretos —art. 197.1 del Código penal—. Pero, en atención al interés protegido, quedarían fuera del ámbito penal, entiendo, las grabaciones que se realicen en un "ámbito no reservado a la intimidad". En este último caso podrían ser constitutivas de un ilícito civil[15].

[15] El artículo 7 de la LO 1/ 82 establece: Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:
1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.
2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.
3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.
5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.

En mi opinión, el criterio general debe ser que, si las grabaciones se realizan por un tercero, pero en un espacio no reservado a la intimidad no cabe exigir responsabilidad penal, aunque sí pueda exigirse responsabilidad en el ámbito civil. La protección penal se reservaría para los casos más graves que serán aquellos que tienen lugar en ámbitos destinados al desarrollo de la vida íntima de las personas. No obstante, lo más frecuente es que, dado que se trata de delitos perseguibles a instancia de parte[16], los afectados acudan a la vía civil incluso ante grabaciones realizadas en lugares que podrían considerarse "no públicos", por lo que es en esta jurisdicción en la que se dirimen la mayoría de los casos, a pesar de que algunos de ellos podrían ser constitutivos de una infracción penal.

En concreto, el Tribunal Constitucional sí ha aceptado la lesión de la intimidad y de la propia imagen en el caso de grabaciones realizadas por terceros en lugares abiertos al público, o

---

6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.
8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas.
Por su parte, el artículo 8 establece:
Uno. No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante.
Dos. En particular, el derecho a la propia imagen no impedirá:
a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.
b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.
c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.
Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

[16] No obstante, el actual "Proyecto de Ley Orgánica de protección integral a la infancia y la adolescencia frente a la violencia" suprime el actual artículo 201 C.P. y, en su lugar, propone la siguiente redacción de dicho precepto:
"1. Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.
2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.
3.[Modificado por LO 5/2010] El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130 de este Código".

al menos no estrictamente privados, pero lo ha hecho en relación con casos dirimidos en el ámbito civil; ahora bien, estas decisiones del Tribunal son imprescindibles como punto de partida para la delimitación del ámbito penal en esta materia, en la medida en que acotan el marco dentro del cual se ha de concretar el objeto de protección penal. De la doctrina actual del Tribunal Constitucional en relación con estos supuestos, reflejada en algunas de sus sentencias, y en las que, como vamos a ver, se opone al criterio defendido por el Tribunal Supremo, paso a ocuparme a continuación.

En su sentencia 19/2014, e l Tribunal Constitucional calificó de infracción del derecho a la propia imagen la difusión de la imagen de una actriz en la playa semidesnuda, que había sido realizada sin su consentimiento por terceras personas; el Tribunal consideró que la emisión de esas imágenes carecía de interés público alguno[17]. En este caso, los órganos judiciales que habían conocido de los hechos en primera instancia habían apreciado vulneración del derecho a la imagen, pero la Sala civil del Tribunal Supremo revocó la decisión por entender que la información publicada tenía interés público: "el propio de los medios pertenecientes al género de entretenimiento, plenamente admitido por los usos sociales, para el que puede ser noticia el físico de una reconocida actriz o su top-less". A juicio del Tribunal Supremo, "el personaje público que en lugar público se expone a la mirada ajena asume que su imagen pueda ser captada y difundida sin su consentimiento, le satisfaga o no el resultado. Por tanto, desde el punto de vista de la proporcionalidad, debe primar la libertad de información"[18].

Pues bien, frente a estos argumentos el Tribunal Constitucional declaró qué la ausencia de consentimiento para la difusión de la imagen es un factor decisivo en la necesaria ponderación de los derechos en conflicto. El derecho a la información, en su opinión, no ocupa una posición prevalente respecto del derecho a la imagen, solo se antepone a este último tras apreciar el interés social de la información publicada como fin constitucionalmente legítimo. Pero a un mismo tiempo indica que la legitimidad de las informaciones que impliquen una intromisión en otros derechos fundamentales requiere no solo que la información sea veraz, sino que su contenido tenga interés general, pues solo en ese caso puede exigirse a aquellos a quienes afecta o perturba el contenido de la información que, pese a ello, la soporten en aras del interés de la formación de la opinión pública, sin que baste a tales efectos la simple satisfacción de la curiosidad ajena. A

[17] STC 19/2014, de 10 de febrero, Sala de lo civil. En este supuesto, la demanda se presentó únicamente por infracción del derecho a la propia imagen.
[18] STS 125/2011 de 25 de febrero, F.J. 4º, Sala de lo civil.

juicio del Tribunal "no cabe identificar indiscriminadamente interés público con interés del público, o de sectores del mismo ávidos de curiosidad. Curiosidad que, lejos de justificar una merma del derecho a la intimidad, es de la que ha de quedar a salvo ese ámbito de reserva personal constitucionalmente protegido". A esta conclusión no puede oponerse —precisa este Órgano judicial— el hecho de que otras publicaciones hubieran divulgado con anterioridad imágenes o informaciones sobre la vida privada de la persona afectada en circunstancias similares[19].

Por su parte, la STC 18/2015, en contra también de lo que había resuelto la Sala de lo civil del Tribunal Supremo, califica de intromisión ilegítima en los derechos a la intimidad y a la propia imagen la realización de grabaciones de imágenes llevadas a cabo por terceros en lugares públicos que posteriormente fueron emitidas y comentadas en programas televisivos[20].

El Tribunal Supremo había considerado que la afectación del derecho a la intimidad y a la propia imagen había sido muy escasa por lo que debía prevalecer el derecho a la libertad de información y expresión. Sus argumentos principales fueron, por un lado, que el reportaje publicado se refería a las relaciones íntimas del afectado con su pareja sentimental, lo que ya había sido objeto de un reportaje público, por lo que los interesados no habían adoptado pautas de comportamiento con el fin de resguardar ese ámbito reservado frente a una publicidad no querida. Y, por otro lado, que se trataba de un personaje público, cuya imagen era objeto de interés y que había sido captada en espacios de público acceso. Bajo tales circunstancias —afirmó el Tribunal Supremo—, la persona pública se ve despojada de su derecho a disponer de la propia imagen y ha de soportar las molestias que pueda causarle la captación y reproducción de su figura física sin su consentimiento[21].

Pues bien, en oposición a estos razonamientos, el Tribunal Constitucional afirmó, por una parte, que el carácter público del lugar donde se obtienen las imágenes no ubica necesariamente al afectado fuera del ámbito de protección inherente al derecho a la intimidad; y, por otra parte, que la información carecía de interés público. Según lo declarado por el Tribunal, ni el hecho de que una persona tenga notoriedad social justifica, sin más, la captación clandestina y posterior publicación en programas televisivos de imágenes referidas al ámbito personal y privado; ni el hecho de que el interesado haya sido proclive a dar a conocer aspectos de su vida privada o que la relación afectiva fuera ya conocida, son circunstancias susceptibles de cercenar el derecho a la

[19] STC 19/2014, de 10 de febrero, FF.JJ. 5º, 6º y 7º.
[20] STC 18/2015, de 16 de febrero, F.J. 5º, con referencia a la STC 7/2014, de 27 de enero y a la STEDH Von Hannover c. Alemania, Gran Sala, de 7 de febrero de 2012.
[21] STS 264/2012, de 18 de abril, F.J. 2º, Sala de lo civil.

intimidad. Y, en cuanto a la relevancia pública de la información, el Tribunal afirma que resulta inconcuso que el contenido de la información revelada a través de las imágenes difundidas queda fuera del ámbito que es propio de los asuntos de relevancia pública: la protección constitucional se ciñe a la transmisión de hechos "noticiables" que por su importancia o relevancia social puedan contribuir a la formación de la opinión pública, sin que la satisfacción de la curiosidad de una parte del público en relación con detalles de la vida privada de una persona pueda considerarse contribución a tal efecto, concluyendo que "no es el titular del derecho a la propia imagen el sujeto obligado a su protección ni quien debe erigir –por así decirlo– obstáculos o barreras defensivas frente a posibles injerencias de terceros, sino que son los terceros quienes vienen constitucionalmente obligados a respetar el derecho fundamental, cuando se trata, como ocurre en el presente caso, de la captación de imágenes que se refieren a un ámbito personal y privado"[22].

Por su parte, la STC 39/2016 sí justificó la instalación por un empresario de cámaras de videovigilancia en el establecimiento comercial, incluida la caja del centro, ante la sospecha —confirmada por las grabaciones— de sustracciones de dinero por parte de una empleada. De la instalación de las cámaras se había dado información general mediante un aviso a la entrada del establecimiento. Las razones esgrimidas por el Tribunal fueron, de un lado, que la finalidad de la instalación de las cámaras era la seguridad o control laboral, lo que entra dentro de las facultades del empresario, siempre que se ejerzan dentro de su ámbito legal y no lesionen los derechos fundamentales del trabajador; y, de otro lado, que el consentimiento se entiende implícito en la propia aceptación del contrato, que implica reconocimiento del poder de dirección del empresario, siempre y cuando se haya observado la obligación de información previa, conforme con lo establecido por la Instrucción dictada por la AEPD, sin que resulte necesario especificar la finalidad exacta asignada a ese control[23].

Las circunstancias concurrentes en este último supuesto presentan claras diferencias con los anteriores. Como argumenta el Tribunal Constitucional, son varias las razones que justifican en este caso la grabación: quien lleva a cabo las grabaciones está autorizado para ello, su actuación entra dentro de sus facultades reconocidas en la legislación laboral; se ha informado previamente a clientes y empleados de la colocación de las cámaras; y la finalidad pretendida con las

[22] STC 18/2015, de 16 de febrero, FF.JJ. 5º y 6º, con referencia a la STC 7/2014, de 14 de enero, F.J. 4º y a la STEDH, de 24 de junio de 2004,(STEDH 2004, 45), caso Von Hannover c. Alemania, §§ 65 y 76.
[23] STC 39/2016, de 3 de marzo. En este caso, el Tribunal desestimó el recurso interpuesto contra el Auto de la Sala de lo social del Tribunal Superior de Justicia de Castilla y León de 23 de octubre de 2013.

grabaciones persigue un interés social legítimo, lo que justifica la afectación de la intimidad que pueda representar en esas circunstancias la grabación.

Una primera conclusión que cabe extraer de todo lo anterior, es que en la ponderación que hace el Tribunal Constitucional entre los derechos a la intimidad y a la propia imagen en su confrontación con el derecho a la información, el peso que otorga a aquellos derechos es mayor al que le otorga el Tribunal Supremo. Este último, como se ha visto, ha defendido en sus resoluciones un ámbito más restringido del derecho a la intimidad y a la propia imagen frente al derecho a la libertad de información. En este punto, y teniendo en cuenta la gran vulnerabilidad de las personas ante el riesgo que representa la posible difusión de aspectos de la vida privada a través del uso de medios tecnológicos como, por ejemplo, las redes sociales, me parece más acertada la ponderación que hace el Tribunal Constitucional. Estamos ante un ámbito en el que la capacidad intrusiva de las llamadas "nuevas tecnologías" es inmensa y la reparación del daño una vez causado es extremadamente difícil.

Pero, como ya he comentado, por razones de proporcionalidad y de intervención mínima, esa extensa protección del derecho a la intimidad debe corresponder al Derecho civil. En consecuencia, en mi opinión, solo las grabaciones realizadas por terceros sin consentimiento de la persona afectada y con ánimo de vulnerar la intimidad, que se lleven a cabo en un lugar reservado a la intimidad y su contenido afecte a la esfera íntima de la vida personal (intimidad en sentido estricto), pueden ser constitutivas de un delito del artículo 197.1 C.P. y su difusión caería bajo el ámbito de aplicación del tipo agravado previsto en el artículo 197.3 C.P.

No obstante, hay dos cuestiones controvertidas. La primera es la ambigüedad existente respecto de lo que deba entenderse por un "ámbito reservado a la intimidad", a pesar de que se trata de un elemento que puede marcar la línea divisoria entre el ilícito civil y el penal. Así, mientras el Tribunal Supremo no ha considerado como un lugar reservado a la intimidad un despacho profesional[24], sin embargo, el Tribunal Constitucional en relación con grabaciones realizadas en las dependencias comunes de un hotel ha apreciado, en un caso dirimido en el ámbito civil, infracción del derecho a la intimidad, por considerar que en tal lugar se desarrolla una "faceta estrictamente reservada de la vida privada". En concreto, el Tribunal Constitucional

[24] Así lo ha entendido la STS 652/2016, de 15 de julio, Sala de lo Penal, F.J. 8º. Para una referencia a otras resoluciones en este mismo sentido del Tribunal Supremo y de Audiencias Provinciales puede verse, Juanatey Dorado, C. y Doval Pais, A.: "Límites a la protección de la intimidad frente a la grabación de conversaciones o imágenes", en Boix Reig, J. (dir.) y Jareño Leal, A. (coord.): *La protección jurídica de la intimidad*, Madrid, 2010, pp. 147-148.

declaró: "hay que rechazar que el carácter accesible al público de algunas dependencias del establecimiento hotelero tenga la capacidad de situar la actuación de los demandados extramuros del ámbito de protección del derecho a la intimidad, pues ante una faceta estrictamente reservada de su vida privada y no existiendo consentimiento expreso, válido y eficaz prestado por los titulares de los derechos afectados, se produce una intromisión ilegítima en sus derechos fundamentales a la intimidad"[25]. También en este caso, el Tribunal Supremo había revocado la decisión de los órganos judiciales inferiores y había juzgado prevalente la libertad de información frente a los derechos a la intimidad y a la propia imagen de los demandantes[26].

La segunda cuestión es la concreción de la intimidad en sentido estricto, es decir, la delimitación de la esfera más íntima de la vida personal. Estamos ante un concepto ambiguo que presenta unos contornos difusos. En principio, un criterio guía podría ser entender que los aspectos relativos al llamado "núcleo duro" de la intimidad se situarían dentro de este subconjunto, que sería la intimidad en sentido estricto (con la legislación actual habría que apreciar en tales supuestos la agravante del artículo 197.5 C.P.). Pero no necesariamente ha de ser así, pues, de un lado, aun tratándose de información o imágenes que afecten a este núcleo es posible que, atendiendo a las circunstancias concretas del caso, por razones de proporcionalidad e intervención mínima, el hecho deba quedar al margen del Derecho penal (por ejemplo, imágenes de la persona rezando en su domicilio). Y, de otro lado, es posible que las imágenes aun no perteneciendo al núcleo duro de la intimidad, puedan afectar a esa esfera más íntima de la vida personal que uno desea mantener al margen del conocimiento de los demás (por ejemplo, una imagen de la persona en un lugar apartado realizando algún tipo de acción en la que, claramente, ni él ni nadie en su lugar desearía ser visto). Es obvio que habrá casos que no presenten dificultades a la hora de incluirlos bajo ese concepto estricto de intimidad, pero habrá otros que puedan presentar dudas. En esta última hipótesis habrá que atender a todas las circunstancias del hecho y a las expectativas razonables de la persona acerca de su privacidad.

El criterio propuesto, como se ha señalado, choca con la existencia de la agravante prevista en el artículo 197.5 C.P. que incrementa la pena de los delitos previstos en los cuatro primeros números del mismo artículo 197, cuando la conducta afecte precisamente a ese núcleo duro de la intimidad. Por ello, *de lege ferenda* lo razonable sería un cambio legislativo que o bien modificase el artículo 197 de manera que se limitase a proteger exclusivamente el núcleo duro de

[25] STC 176/2013, de 21 de octubre, F.J. 7º.
[26] STS 719/2009, de 16 de noviembre.

la intimidad, eliminándose la agravante del artículo 197.5[27], o bien que suprimiese la agravante, pero dejando a la valoración judicial, debidamente motivada, la determinación de la gravedad de la afectación de la intimidad y la fijación de la pena entre el máximo y el mínimo del marco legal concreto. Quizás la primera opción sería la más coherente con el principio de legalidad, aun a costa de dejar fuera algún supuesto que no afectando al núcleo duro de la intimidad, pueda ser un atentado grave a este derecho. Para estos casos, más bien excepcionales, quedaría la vía civil.

Todo lo anterior significa que la valoración sobre si las grabaciones realizadas por terceros suponen una vulneración del derecho a la intimidad relevante penalmente requiere, en todo caso, un juicio de ponderación específico que atienda, entre otras cosas, a la forma y al lugar en el que se obtengan las grabaciones de la imagen o del sonido, y al contenido de las mismas. De manera que, las cosas estarán claras si las grabaciones realizadas con ánimo de vulnerar la intimidad se hacen con un teleobjetivo en las duchas de un polideportivo y afecten a aspectos íntimos de la persona, por ejemplo; pero las dudas surgirán en aquellas hipótesis como las de las dependencias comunes de un hotel o incluso el domicilio si el contenido de la grabación no tiene que ver con el ámbito más íntimo de la persona (por ejemplo, se ve a la persona cocinando o leyendo en un sillón). En estas últimas situaciones, es difícil saber cuál sería la respuesta del Tribunal Constitucional acerca de la constitucionalidad de la intervención penal. Desde mi punto de vista, la respuesta penal debería estar reservada para los casos más graves, esto es, los mencionados en primer lugar, y en los casos dudosos, como los mencionados en segundo lugar, en principio, debería optarse por la vía civil.

3. Grabación de conversaciones o de escenas por parte de quien participa en las mismas, pero con el desconocimiento del otro u otros participantes; esto es, grabación subrepticia de conversaciones o escenas "con otros"[28].

Las grabaciones "con otros", al realizarse con el desconocimiento de las personas grabadas es evidente que afectan al poder de control que para su titular caracteriza a los derechos a la intimidad y a la propia imagen. Sin embargo, el hecho de que la grabación se realice por una

[27] En este orden de cosas, la STS 476/2020, de 25 de septiembre, ya establece que el ámbito de protección del artículo 197.2 se reduce al núcleo duro de la intimidad y rechaza la aplicación de la agravante del artículo 197.5 por considerar que lo contrario vulneraría el *ne bis in idem.*

[28] Grabaciones "con otros" es la denominación que dio a estos supuestos el Tribunal Constitucional para distinguirlos de las grabaciones "de otros" cuando es un tercero ajeno a la conversación o a la escena quien realiza la grabación (STC 114/1984, de 29 de noviembre, F.J. 7º).

persona que participa en la conversación o en la escena ha dado lugar a una controvertida doctrina jurisprudencial. La cuestión que se ha planteado en todos estos supuestos de grabaciones "con otros" es si puede hablarse de ausencia de consentimiento. Un supuesto paradigmático es el de la utilización de cámaras ocultas por parte de uno de los participantes en la escena —en la mayoría de los supuestos, periodistas de investigación—, que con posterioridad difunde o publica esas conversaciones o esas imágenes sin el consentimiento de las personas grabadas, afectando de ese modo a sus derechos.

Procederé a analizar separadamente cuál ha sido el tratamiento jurisprudencial de estos casos según se trate de grabaciones de conversaciones o de escenas[29]:

a) En el caso de grabación de conversaciones, la línea jurisprudencial seguida por los tribunales durante muchos años ha sido considerar, por un lado, que "no hay «secreto» para aquel a quien la comunicación se dirige" y, por tanto, que no hay vulneración del derecho al secreto de las comunicaciones; todo ello, con base en la fundamental sentencia del Tribunal Constitucional, 114/1984[30] que constituye una clara referencia en esta materia[31]. Y, por otro lado, que quien habla con otro *se despoja* de su intimidad y, en consecuencia, este otro puede usar el contenido de la conversación sin reproche jurídico alguno, por lo que tampoco habría lesión del derecho a la intimidad[32]. Esta fue la doctrina jurisprudencial mantenida con respecto a la conducta de *grabar* tanto en el orden civil como en el penal[33]. A pesar de ello, en alguna ocasión la Sala 1ª del Tribunal Supremo entendió que la *publicación* de la conversación obtenida constituía un ataque contra la intimidad porque, como afirmó el Tribunal, "es esa actuación «ad extra» y no el propio registro lo que configura el efectivo ataque a la intimidad"[34].

---

[29] En trabajos anteriores con Doval Pais nos ocupamos de analizar la jurisprudencia de las salas civil y penal del Tribunal Supremo, así como algunos pronunciamientos de audiencias provinciales y pudimos apreciar un diferente tratamiento de los casos según se tratase de grabación de conversaciones o de escenas. El resultado de este análisis puede verse en Juanatey Dorado, C. y Doval Pais, A.: "Límites a la protección…", ob. cit., pp. 127-169; y en Doval Pais, A. y Juanatey Dorado, C.: "Consecuencias jurídicas del uso de cámaras ocultas y problemas de la STC 12/2012, de 30 de enero", en Anarte Borrallo, E., Moreno Moreno, F. y García Ruiz, C.: *Nuevos conflictos Sociales. El papel de la privacidad*, Madrid, 2015, pp. 219-240.

[30] STC 114/1984, de 29 de noviembre, F.J. 7º.

[31] Pueden verse, por todas, las STS 883/1994, de 11 de mayo, F.J. 3º; 2081/2001, de 9 de noviembre, F.J. 9º; 1051/2009, de 28 de octubre, F.J. 2º; 682/2011, de 24 de junio, F.J. 6º; y 298/2013, de 13 de marzo, F.J. 1º.

[32] Véanse, entre otras, las SSTS 238/1996, de 1 de marzo, F.J. 1º y 1354/2005, de 16 de noviembre, F.J. 2º.

[33] Una extensa referencia a esta jurisprudencia puede verse en Juanatey Dorado, C. y Doval Pais, A.: "Límites a la protección…", ob. cit., pp. 135-143.

[34] SSTS, Sala de lo civil, 1168/2000, de 22 de diciembre, F.J. 1º, y 1079/2001, de 13de noviembre, FF.J.J. 2º y 3º.

En la última década podría decirse que la anterior jurisprudencia ha sido en cierta medida matizada, al menos de forma explícita. El punto de partida sigue siendo el mismo: no hay secreto para aquél a quien la comunicación se dirige, ni implica contravención del artículo18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje; no hay afectación del derecho al secreto de las comunicaciones ni del derecho a la intimidad cuando una persona graba sus propias conversaciones con terceros. Sin embargo, de esta regla general se excluyen expresamente los supuestos de grabaciones "con otros" que se utilizan como un medio de provocación al delito o cuando se emplean como medio de indagación desde estructuras oficiales de investigación delictiva (de manera que no podrán utilizarse como prueba en el proceso penal), pero también se excluyen aquellas grabaciones en las que su contenido afecte "al núcleo esencial de la intimidad personal o familiar de uno de los interlocutores"[35], así como "los supuestos en los que el contenido de lo grabado es divulgado, ocasionando un daño a la intimidad para lo que habría de estarse al contenido, íntimo o no, de lo que se divulga y ha sido obtenido de forma irregular" [36].

En resumen, el Tribunal Supremo declara, por un lado, la ilicitud de las grabaciones "con otros" (que no se ven amparadas por el derecho al secreto de las comunicaciones) si se utilizan como medio de provocación al delito o como un instrumento para la investigación delictiva, pero lo hace únicamente en orden a inadmitir el contenido de las grabaciones como prueba en el contexto del proceso, pero no para determinar si cabe en esos casos apreciar infracción del derecho al secreto de las comunicaciones del artículo 7 de la LO 1/82, o del artículo 197.1 C.P.

Por otro lado, afirma que la lesión de la intimidad se produce no solo con la *divulgación* de lo grabado "con otros" sin su consentimiento, sino también con el hecho mismo de la *grabación*, si afecta al núcleo esencial de la intimidad, aunque esto último también lo dice exclusivamente en el contexto del proceso a los efectos de admitir o no las grabaciones como prueba. Por lo que tampoco en este caso queda claro si, en su opinión, cabría o no, en su caso,

---

[35] STS 214/2018, de 8 de mayo, F.J. 2º, Sala de lo penal.

[36] STS 214/2018, de 8 de mayo, F.J. 2º, Sala de lo penal, con referencia a la STS 652/2016, de 15 de julio. En esta última resolución el Tribunal afirma que, si bien la divulgación a terceros del contenido de la grabación "con otros" podría vulnerar el derecho a la intimidad, para ello sería preciso que la conversación tuviera un contenido que afectara al núcleo esencial del derecho a la intimidad, ya sea en su ámbito personal o en el familiar. Sin embargo, la entrevista grabada se desarrolló en el despacho profesional de uno de los interlocutores y no tenía nada que ver con el ámbito de la intimidad personal en ninguna de sus modalidades, sino con un tema empresarial que aparecía contaminado por una actuación previa ilícita consistente en la petición de dinero por parte de los acusados a los empresarios a cambio de una concesión (F.J. 8º).

infracción del derecho a la intimidad del artículo 7 de la LO 1/82, o del artículo 197.1 C.P. por el hecho de grabar, aunque parecería que no.

En definitiva, de la doctrina jurisprudencial existente sobre la cuestión lo que cabe extraer es que a lo que se da relevancia no es tanto a si hay o no consentimiento, que parece partirse de que sí lo hay, sino a la esfera de la intimidad que se ve afectada. Sin embargo, desde mi punto de vista, no se puede afirmar sin más que estas grabaciones sean consentidas. En mi opinión, hay supuestos que pueden merecer una respuesta penal y eso implica aceptar que tales grabaciones "con otros" no son consentidas A ello aludiré más adelante.

b) Y, por lo que concierne a la grabación subrepticia de imágenes por un participante en la escena, tanto la Sala civil como la penal del Tribunal Supremo, en un primer momento, sostuvieron que, por las mismas razones aducidas en el caso de la grabación de conversaciones, no hay vulneración del derecho al secreto de las comunicaciones, ni del derecho a la intimidad, aunque con respecto a este último derecho con algunos matices. De acuerdo con la doctrina mantenida inicialmente por el Tribunal Supremo, no cabe apreciar infracción de estos derechos cuando la persona que es objeto de la grabación ha exteriorizado sus pensamientos o actos sin coacción de ninguna especie[37]; la persona, en este caso —entiende el Tribunal—, se despoja voluntariamente de sus intimidades: lo que graba quien participa en la escena es lo que el otro exhibe y dice; es decir, lo que ve con sus ojos y lo que oye con sus oídos y, por tanto, la grabación en modo alguno infringe la intimidad ni ningún otro derecho de la persona que es grabada sin *su* conocimiento[38]. No obstante, en alguna ocasión, lo que se deduce "a contrario sensu" de las afirmaciones del Tribunal es que cabría apreciar violación de la intimidad si la grabación de las imágenes hubiese tenido lugar en un "*ámbito reservado a la intimidad*"[39]. Esto es, si las imágenes

[37] STS 883/1994 de 11 de mayo, F.J. 3º y STS 1100/2001, de 8 de junio, F.J. 1º, ambas de la Sala de lo penal. Aquí podría comentar los hechos: empresa de cobro de morosos

[38] STS 178/1996, de 1 de marzo, F.J. 1º. En esta resolución el Tribunal declara. "la validez de una grabación subrepticia de una conversación entre cuatro personas realizada por una de ellas sin advertírselo a los demás, no ataca a la intimidad ni al derecho al secreto de las comunicaciones, ya que las manifestaciones realizadas representaban la manifestación de voluntad de los intervinientes que fueron objeto de grabación de manera desleal desde el punto de vista ético pero que no traspasan las fronteras que el ordenamiento jurídico establece para proteger lo íntimo y secreto". Pero, a un mismo tiempo, el Tribunal rechaza la validez de la grabación como medio de prueba en el proceso pues ello supondría a su juicio desconocer el derecho de los acusados a no declarar contra sí mismos y a no confesarse culpables.

[39] STS de 977/1999, de 17 de junio, Sala de lo penal, F.J. 1º. En este caso se consideró que el aula de audiovisuales de una escuela no es un ámbito reservado a la intimidad. Los hechos analizados en esta sentencia, que resulta de particular interés fueron los siguientes: un menor, de 16 años de edad, estaba siendo objeto de acoso por parte de un profesor. En una de las ocasiones en las que el menor fue citado por el profesor en el aula de audiovisuales de la escuela, con el pretexto de hacer un futuro examen que luego el profesor sustituiría por el original, el alumno decidió llevar consigo una grabadora de video con la que

son obtenidas en un ámbito reservado a la intimidad, parece que ya no valdría el argumento de que la persona se despoja de su intimidad y, en consecuencia, sí se admitiría la infracción de este derecho.

Sin embargo, la sentencia del Pleno de la Sala de lo Civil del Tribunal Supremo, de 16 de enero de 2009, se apartó de esta doctrina y sentó una nueva línea jurisprudencial. Muy resumidamente, los hechos juzgados en esta resolución consistieron en la grabación y posterior emisión en un programa de televisión de las imágenes captadas mediante una cámara oculta en la consulta de una esteticista y naturista; las grabaciones las llevó a cabo una periodista que se hizo pasar por una clienta potencial. Aunque los órganos judiciales inferiores habían desestimado la demanda interpuesta por la titular de la consulta, el Tribunal Supremo sí apreció infracción de los derechos a la intimidad y a la propia imagen por considerar que la grabación y la emisión de las imágenes no habían sido consentidas. A juicio del Tribunal, la conducta no podía entenderse justificada por el interés en descubrir (y comunicar) la verdad de lo que acontecía en la consulta, pues hubiese bastado a tal efecto —afirmó— realizar entrevistas a los clientes[40]. Esto es, la medida se consideró desproporcionada por innecesaria y, por tanto, el Tribunal acepta el uso de la cámara oculta pero con límites[41].

Esta sentencia fue recurrida ante el Tribunal Constitucional que no solo la confirmó sino que afirmó: "Aun cuando la información hubiera sido de relevancia pública, los términos en que se obtuvo y registró, mediante el uso de una cámara oculta, constituyen en todo caso una ilegítima intromisión en los derechos fundamentales a la intimidad personal y a la propia imagen", que se desarrolló en un ámbito indudablemente privado, por lo que "es forzoso concluir que hubo una intromisión ilegítima en el derecho fundamental a la intimidad personal". E incluso llega a la tajante conclusión de que "tuviese o no relevancia pública lo investigado por el periodista, lo que

grabó cómo el profesor, tras cerrar la puerta de la sala, proyectaba una película de contenido "pornográfico", al tiempo que procedía a masturbarse ante el alumno y le pedía que tocase su pene por dos veces a lo que el joven se negó y salió del lugar. El Tribunal consideró válida la prueba.

[40] Los pronunciamientos posteriores de la Sala de lo Civil del Tribunal Supremo han seguido, en general, la importante directriz establecida por la Sentencia del Pleno del TS de 16-1-2009. Con referencias a esta doctrina véanse, entre otras, las SSTS, Sala de lo Civil, 536/2009, de 30 de junio, F.J. 4º; 506/2009, de 6 de julio, F.J. 2º; 378/2011, de 6 de junio, F.J. 9º; y 225/2014, de 29 de abril, FF.JJ. 7º y 8º.

[41] Como resume la STS 225/2014, de 29 de abril, Sala de lo Civil: "se admite que el uso de la cámara oculta pueda ser legítimo cuando lo justifique el interés público en el conocimiento de los hechos y ese medio sea imprescindible para obtener la información y, además, proporcionado para que la lesión de los derechos fundamentales sea la menor posible "(F.J. 7º); Véase, Doval Pais, A. y Juanatey Dorado, C.: "Consecuencias jurídicas…", ob. cit., p. 224.

está constitucionalmente prohibido es justamente la utilización del método mismo (cámara oculta)"[42].

La contundencia de tales afirmaciones podrían llevar a entender que, a juicio del Tribunal, si la grabación tiene lugar en un ámbito privado, debido a la especial capacidad intrusiva del uso de una cámara oculta, ello implicará siempre la lesión de la intimidad y de la propia imagen. Y ello con independencia de la relevancia pública de lo investigado. Esto es, una prohibición absoluta del uso de cámaras ocultas.

En un trabajo anterior con Antonio Doval ya consideramos que esta resolución debía ser entendida en atención a las circunstancias que rodearon la grabación realizada en ese supuesto específico, sin que tal decisión significase la ilicitud general y absoluta de toda grabación realizada con cámara oculta[43].

Pues bien, efectivamente, el Tribunal Constitucional en su sentencia 25/2019, de 28 de febrero, matiza su anterior resolución y afirma que la utilización de un dispositivo oculto de captación de la voz y de la imagen se basa en un ardid o engaño que impide a la persona que está siendo grabada ejercer su legítimo poder de control, con el agravante de que tales grabaciones, normalmente, van a ser difundidas por medios tecnológicos cuya capacidad expansiva es inmensa. El Tribunal subraya que la inexistencia de consentimiento expreso, válido y eficaz a la cámara oculta es lo que propiamente conforma una injerencia en los derechos a la intimidad y a la propia imagen y, por consiguiente, origina la situación de conflicto de derechos fundamentales que requiere para su resolución un juicio de ponderación entre los mismos. Y concluye su argumentación afirmando que la libertad de información puede ser considerada prevalente solo si la información es veraz y relevante para la formación de la opinión pública, sobre asuntos de interés general y en la medida en que se desenvuelva dentro de ese marco; de manera que, una vez confirmada la existencia de la relevancia pública de la información, el uso periodístico de la cámara oculta requiere, según el Tribunal, un juicio específico de proporcionalidad que valore no solo la forma y el lugar en el que se obtengan las grabaciones, sino también el modo en que se difundan posteriormente y la existencia o no de medios menos intrusivos para obtenerla[44].

---

[42] STC 12/2012, de 30 de enero. F.J. 7º.

[43] La prohibición absoluta no es coherente con la línea jurisprudencial consolidada del Tribunal Constitucional que afirma que "ningún derecho protegido constitucionalmente goza de protección absoluta" (STC 53/85, de 11 de abril, F.J. 9º). Sobre el tema puede verse, Doval Pais, A. y Juanatey Dorado, C.: "Consecuencias jurídicas…", ob. cit., pp. 224-240.

[44] STC 25/2019, de 28 de febrero, F.J. 7º. Véase también la STC 58/2018, de 4 de junio, F.J. 7º

Aunque el Tribunal Constitucional en esta última sentencia se refiere a supuestos de utilización de cámaras ocultas por parte de periodistas, es evidente que sus argumentos son aplicables a toda grabación "con otros" realizada por medio de cualquier instrumento tecnológico de grabación y por parte de cualquier persona sea o no periodista.

En consecuencia, admitida la ausencia de consentimiento y la posible infracción del derecho a la intimidad, la cuestión está en valorar si esa infracción puede ser sancionable con arreglo al artículo 197.1 C.P., cuando la grabación se realice en un espacio reservado a la intimidad y pueda afectar a aspectos verdaderamente íntimos de la persona. En mi opinión, puesto que la grabación no es consentida, sí cabría responsabilidad penal, aunque, de nuevo, el problema está en determinar si el lugar en el que se lleva a cabo la grabación es un lugar reservado a la intimidad o no. Como hemos visto, mientras que el Tribunal Supremo ha considerado que un despacho profesional no lo es, el Tribunal Constitucional lo ha calificado de ámbito indudablemente privado. Por eso, creo que lo verdaderamente importante no es si es un despacho profesional o una sala de audiovisuales, lo relevante penalmente es que sea un lugar que en el momento de los hechos no sea accesible al público, esto es, ha de tratarse de un ámbito en el que haya una clara la expectativa de privacidad[45], y que el contenido de lo que se graba afecte a aspectos verdaderamente íntimos de la persona (por ejemplo, grabación de una relación sexual "con otro", en su despacho, sin su consentimiento).

4. Posición personal

Todo lo anterior me permite extraer las siguientes conclusiones:

En primer lugar, las grabaciones de conversaciones o de imágenes por una tercera persona sin el consentimiento de quienes participan en esa conversación o en la escena grabadas, en principio, podrían ser constitutivas de un delito de descubrimiento y revelación de secretos, salvo que se lleven a cabo en un "lugar no reservado a la intimidad". De modo que, si la conducta tiene lugar en un ámbito "no reservado a la intimidad" debe excluirse, como he señalado, la

[45] En este sentido el Tribunal Constitucional ha declarado que un criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de "las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno", SSTC 12/2012, de 30 de enero, F.J. 5º y 25/2019, de 28 de febrero, F.J. 4º.

responsabilidad penal, pero eso no significa que no pueda haber una intromisión ilegítima en este derecho[46]. En los casos dudosos, solo un conocimiento de todas las circunstancias del hecho permitirán determinar si se trata o no de un "ámbito reservado a la intimidad", lo que ha de valorarse en atención a las expectativas razonables de privacidad. Pero, además, desde mi punto de vista, es necesario que el contenido de lo grabado afecte a la esfera más íntima de la persona, solo así se puede justificar la intervención del Derecho penal.

En segundo lugar, en los casos de grabaciones de la voz o de la imagen "con otros", sin el asentimiento de la persona grabada, no hay vulneración del derecho al secreto de las comunicaciones, pero eso no significa la inexistencia de infracción del derecho a la intimidad de la persona cuya imagen o voz son grabadas sin su conocimiento[47]. Y, puesto que la acción de grabar no es consentida, entiendo que sí cabría responsabilidad penal si la grabación se realiza con ánimo de descubrir los secretos ajenos o de vulnerar la intimidad de otro, se lleva a cabo en un lugar reservado, el contenido afecta a la esfera íntima de la persona y la grabación no se puede amparar en la libertad de información por carecer el contenido de la misma de interés público. Y, en consecuencia, de acuerdo con la actual regulación penal, la divulgación del contenido de la grabación en tales hipótesis caería bajo el supuesto agravado previsto en el artículo 197.2 C.P.

En mi opinión, existe un plus importante, desde el punto de vista de la pérdida de control sobre los aspectos de la intimidad, entre mantener una conversación o relación íntima con otro y permitir su grabación. Se trata de una grabación subrepticia del sonido o de la imagen y, por consiguiente, una intromisión ilegítima en la intimidad, aunque no suponga vulneración del secreto de las comunicaciones. Cuando alguien cuenta un secreto a otro o mantiene con él una relación íntima, cuenta con la posibilidad de que esa otra persona pueda comportarse deslealmente y, a pesar de ello, lo dice o lo hace; igual que quien escribe una carta en la que cuenta un secreto,

---

[46] Por ejemplo, una discoteca no podría calificarse de "ámbito reservado a la intimidad" y, sin embargo, la Sala de lo civil del Tribunal Supremo calificó de intromisión ilegítima en la intimidad la realización de fotografías de determinadas personas en dicho lugar, STS 780/1993, de 17 de julio, F.J. 2º. Defiende la posible realización de actividades privadas en lugares públicos Valeije Álvarez (en "Intimidad y difusión de imágenes sin consentimiento", cit., pág. 1877).

[47] En este sentido, Jareño Leal, a pesar de que acepta que estas grabaciones se realizan "sin consentimiento", sin embargo, puntualiza que para poder aceptar la posible aplicación del art. 197.1 del Código penal, esto es, para admitir la relevancia penal de la conducta, debe comprobarse si hay efectiva lesión de la intimidad. En su opinión, si no se trata de un contexto relativo a una faceta de la intimidad, puede decirse que no existe base suficiente para la intervención penal (la autora está comentando la STS de 8-06-2001, en la que se produce la grabación con cámara oculta de una entrevista, realizada por una periodista, al gerente de una empresa de cobro de morosos, entrevista que posteriormente fue difundida en un programa de televisión) (en *Intimidad e imagen*, cit., págs. 99-100).

conoce la posibilidad de que esa carta de su puño y letra pueda llegar a conocimiento de terceras personas. Podríamos decir, por eso, que ese riesgo es inherente a esa forma de comunicar un secreto; pero la grabación no es un riesgo inherente al hecho de contarlo o de mantener una relación; en este caso hay una mayor indefensión.

Parece obvio que frente a lo grabado se es más vulnerable, no solo por el uso que pueda hacer el propio sujeto que graba (por ejemplo, mediante la difusión a través las redes sociales), sino porque la existencia de esa grabación genera un grave peligro para la intimidad muy superior al que se genera por el mero hecho de poder contarlo. La grabación puede caer en manos de terceros que pueden hacer un uso perjudicial de la misma[48]. El nuevo artículo 197.7 vendría a confirmar esta tesis que, en definitiva, responde a las mismas razones que han llevado al legislador a tipificar la conducta de revelación, cesión o difusión de grabaciones audiovisuales obtenidas "con consentimiento" y en lugares fuera del alcance de terceros (lugares reservados a la intimidad) y siempre que se produzca un menoscabo grave de la intimidad personal. De este último delito, me ocuparé a continuación.

Por tanto, en supuestos de grabaciones "con otros" hay afectación de la intimidad, pero este derecho puede ceder, en su caso, ante la existencia de un interés público en el conocimiento de lo grabado. Por ejemplo, en atención al interés del Estado en conocer los propósitos –o actos– delictivos y en proteger a la víctima de los mismos.

En conclusión, la conducta de quien graba sin el conocimiento del otro participante ha de considerarse una intromisión ilegítima en la intimidad que puede ser relevante penalmente, aunque, en algunos casos, pueda justificarse en atención a la necesaria protección de otros

---

[48] . De hecho, esto es lo que sucedió en un caso en el que la grabación subrepticia de las relaciones sexuales secretas mantenidas con una persona, cayó accidentalmente en manos de terceros, que pudieron ver las imágenes captadas. En este caso, se condenó por delito de descubrimiento y revelación de secretos (SAP de Lugo de 29-12- 2000). Los hechos analizados en este sentencia fueron los siguientes: el acusado había grabado subrepticiamente con una cámara de vídeo, colocada dentro de un armario, sus relaciones sexuales mantenidas con una mujer con la que tenía una relación que, por expreso deseo de ambos interesados, llevaban en secreto. Con posterioridad, el acusado pidió a un amigo que le realizase una copia en formato que permitiese su visualización en un vídeo doméstico. El amigo lo hizo y guardó la cinta en su domicilio, antes de entregársela al acusado. En ese lapso, el hijo de aquél encontró la cinta y se reunió en su casa con varios amigos, todos ellos menores de edad, y vieron el vídeo. La Audiencia condenó al acusado por un delito de descubrimiento y revelación de secretos (aunque aplicó el Código penal de 1973 por resultar más beneficioso para el reo), por considerar que se trataba de una grabación "sin el consentimiento" de la afectada, que vulneraba su derecho a la intimidad personal. En este caso, el hecho de que el acusado fuese precisamente uno de los participantes en la conducta grabada no fue tenido en cuenta a efectos de rechazar la existencia de una intromisión ilegítima en la intimidad, a pesar de que también en ese supuesto podría defenderse, como hizo el Tribunal Supremo en la sentencia de 17-6-1999, que el "destinatario" en este caso es quien hace uso de la cámara (art. 7 L.O. 1/1982).

intereses en juego[49]. En tales supuestos, estaríamos no en el ámbito de la ausencia de afectación de la intimidad, sino en el de la posible justificación de tal afectación.

IV. Revelación no consentida de imágenes o grabaciones obtenidas con la anuencia de la persona afectada

Estos supuestos presentan una notable diferencia con los previstos en el anterior epígrafe III y es que aquí las grabaciones audiovisuales han de haber sido obtenidas con el consentimiento de la persona afectada, pero la particularidad significativa de este supuesto es que ese consentimiento se otorga —ya sea de forma explícita o implícita— para un uso privado y, sin embargo, posteriormente, una de las partes implicadas en la grabación la difunde sin el consentimiento de la otra. No hay duda de que este es un caso en el que puede haber un menoscabo muy importante de la intimidad y de la imagen que no es consentida, salvo que se entienda —lo que el nuevo delito del artículo 197.7 ya no permite— que quien consiente la grabación consiente cualquier uso que pueda hacerse de ella.

Hasta la reforma del Código penal efectuada por la LO 1/ 2015[50], que introdujo el artículo 197.7 C.P., se entendía mayoritariamente que todos estos casos, cada vez más frecuentes en la práctica, al haber consentimiento de la víctima para la obtención de las imágenes o de las grabaciones, quedaban fuera de la protección penal de la intimidad[51]; y ello a pesar de que podrían llegar a ser más graves desde el punto de vista de la afectación de este derecho, que aquellos otros en los que la grabación la realiza un tercero sin el consentimiento de los participantes en la escena. La gravedad dependerá del contenido de la grabación y del uso que pueda hacerse de ella. No es lo mismo la difusión no consentida en redes sociales de una grabación obtenida con la anuencia

[49] Parece que ésta sería también la opinión de Muñoz Conde quien defiende que la grabación secreta de actos de la intimidad realizada por uno de los participantes es constitutiva de un delito contra la intimidad del art. 197.1 del Código penal. El problema, a su juicio, se centra en si tal conducta delictiva podría quedar amparada por una causa de justificación –estado de necesidad o ejercicio legítimo de un derecho-, en el caso de particulares que graban con la intención de defender sus legítimos intereses, fundamentalmente en el caso de víctimas de un delito que con la grabación pueden ayudar a la identificación del autor y a su consiguiente sanción. En estos supuestos admite que pueda otorgarse valor probatorio a tales grabaciones que considera no consentidas y secretas –aunque las realice uno de los participantes- (en "Prueba prohibida y valoración de las grabaciones audiovisuales en el proceso penal", en *Revista Penal,* núm. 14, págs. 109-115).

[50] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal.

[51] Doval Pais, A. y Anarte Borrallo, E.: "Delitos contra la intimidad…", ob. cit., p. 527.

de la persona interesada durante una fiesta de cumpleaños privada, en la que no se aprecien aspectos verdaderamente íntimos de las personas, que la difusión de una grabación de una relación sexual.

Pues bien, tras la introducción del artículo 197.7 C.P. por la LO 1/2015, en general, la revelación o difusión de grabaciones de la voz o de la imagen que han sido obtenidas por uno de los participantes en la conversación o escena y que han sido consentidas para un uso exclusivamente privado únicamente podrán ser objeto de reclamación por la vía civil (art. 7, LO 1/82)[52]; pero algunos de estos supuestos, especialmente graves, caerán bajo el ámbito de aplicación del artículo 197.7 del Código penal. Este precepto establece:

"*Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menos cabe gravemente la intimidad personal de esa persona.*

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

La introducción de este tipo penal ha dado lugar a una controversia doctrinal entre quienes afirman que este precepto supone una intervención penal excesiva que vulnera los principios de proporcionalidad y de intervención mínima, y aquellos otros que defienden la necesidad de regular penalmente estas conductas debido a su gravedad desde el punto de vista de la afectación del derecho a la intimidad. A mi juicio, este tipo penal viene a cubrir un vacío legal que dejaba fuera de la intervención penal conductas que pueden menoscabar de forma profunda la intimidad. Pero debe ser interpretado de forma restrictiva y aplicado a comportamientos verdaderamente graves.

La conducta consiste en difundir, revelar o ceder a terceros, lo que significa que ha de suponer un traspaso de las imágenes o grabaciones a terceras personas no presentes en las escenas correspondientes. La conducta de difusión es la que conlleva una mayor afectación al bien jurídico en la medida en que implica su distribución a un amplio número de personas (por medio de las redes sociales, correo electrónico, la televisión, mensaje de móvil, etc.). La cesión o la revelación

[52] Como hemos visto, el Tribunal Constitucional ha aceptado la infracción del derecho a la intimidad en casos de estas características.

no requieren necesariamente su traspaso a un amplio número de personas, bastaría con una cesión o revelación a varias o incluso solo a una.

En relación con esto, el Tribunal Supremo ha afirmado que mientras que el vocablo "difundir" ha de entenderse como sinónimo de extender, propagar o divulgar a una pluralidad de personas, las expresiones "revelar" o "ceder" son perfectamente compatibles con una entrega restringida a una única persona. Y, en concreto, ha señalado que el requisito de la difusión queda cumplido cuando, sin autorización de la persona afectada, se inicia la cadena de difusión, siendo indiferente que la imagen sea remitida a una o más personas[53]. Este fue el argumento que empleó para considerar subsumible bajo este tipo penal el envío sin autorización de la foto de una exnovia, en la que estaba desnuda, al compañero sentimental de esta; la fotografía había sido enviada por la mujer a su exnovio anteriormente.

En mi opinión, si la cesión es a una única persona habría que ver si la respuesta penal resulta o no desproporcionada: la cesión a una sola persona puede no representar un daño importante a la intimidad, salvo que eso se traduzca en una pérdida de control sobre la imagen o la grabación que genere un riesgo muy alto de mayor afectación. Todo esto ha de ser tenido en cuenta a la hora de valorar la gravedad del menoscabo de la intimidad personal, lo que podría llevar, en su caso, a la inaplicación del precepto por la ausencia de este elemento típico. De hecho, en lo que parece un *lapsus* del legislador, el propio precepto al referirse a la gravedad del menoscabo alude únicamente a la divulgación.

El tipo penal, además, requiere que lo que se difunda, ceda o revele sean imágenes o grabaciones audiovisuales. Esto es, lo que realmente importa es que se trate de imágenes. Las grabaciones de sonido quedarían fuera del tipo penal, aunque aludan a aspectos verdaderamente íntimos de la persona. De nuevo, tras esta opción, está la apreciación de que son las imágenes las que pueden dañar de forma grave la intimidad de la persona. Y, desde luego, por razones de coherencia y proporcionalidad, deben considerarse incluidas tanto las imágenes captadas por quien las revela, cede o difunde como las recibidas de la persona o personas afectadas, a pesar de que la dicción literal podría llevar a entender que solo serían relevantes penalmente las mencionadas en primer lugar. Así lo ha entendido el Tribunal Supremo que ha declarado que la obtención de las imágenes puede tener muy diferentes orígenes: obtiene la imagen —afirma— tanto quien fotografía o graba el vídeo en el que se exhibe algún aspecto de la intimidad, como quien la recibe cuando es remitida voluntariamente por la víctima valiéndose para ello de

[53] STS 70/2020, de 24 de febrero, F.J. 2º.

cualquier medio convencional o de un programa de mensajería instantánea que opere por redes telemáticas[54].

Y, en particular, en relación con esto, el Tribunal Supremo ha indicado que la exigencia típica de que las imágenes hayan sido obtenidas en un domicilio o en cualquier otro lugar fuera del alcance de terceros debe interpretarse como la pretensión del legislador, si bien expresada con una deficiente técnica legislativa, de subrayar y reforzar el valor excluyente de la intimidad; e, igualmente, la exigencia de que la obtención se verifique "fuera del alcance de terceros", no debe excluir, de acuerdo con el Tribunal, aquellos supuestos en los que la imagen captada reproduzca una escena con más de un protagonista.

El hecho de que el tipo penal requiera que se actúe sin autorización significa que el mero hecho de haber obtenido o captado las imágenes o escenas audiovisuales con el consentimiento de las personas implicadas no permite presumir que ese consentimiento alcanza a una posible revelación, cesión o difusión posterior; al contrario, la presunción es en contra y solo si hay autorización se excluirá el tipo penal. Hay que tener en cuenta que estamos hablando de imágenes o grabaciones que han de suponer una muy grave afectación de la intimidad, que una vez reveladas o difundidas es verdaderamente difícil la reparación del daño.

El tipo requiere, además, que se produzca un grave menoscabo de la intimidad personal. De tal forma que, para valorar la gravedad deberán tenerse en cuenta aspectos como: el lugar en el que se haya llevado a cabo la obtención de la grabación o de la imagen y las expectativas de privacidad que conlleve dicho lugar, en atención a la hora, las mayores o menores facilidades para el acceso de terceras personas y, en general, todas las vicisitudes que rodeen el hecho; el contenido de la revelación y sus consecuencias para la persona desde el punto de vista de su intimidad; así como el alcance de la revelación bien por el número de personas a las que se les ha traspasado o por la cualidad de esas personas. Este es un elemento fundamental del precepto que debe ser interpretado de forma restrictiva, de manera que solo los casos verdaderamente graves generen responsabilidad penal. Es cierto que es una cláusula valorativa indeterminada, pero el bien jurídico intimidad tiene contornos difusos, dependientes de muy diversas circunstancias que pueden concurrir en el hecho y que pueden ser determinantes de la gravedad.

[54] STS 70/2020, de 24 de febrero, F.J. 2º. El hecho de que hubiese sido la propia víctima la que había enviado la foto previamente a quien luego la envía a un tercero, sin su autorización, no impidió al Tribunal Supremo la aplicación del tipo penal.

Para terminar, me parece interesante resaltar que, a diferencia de lo que sucede con los casos analizados en el epígrafe III, que se han dilucidado preferentemente en la vía civil, la vía elegida por los afectados por casos, en principio, recogidos bajo el artículo 197.7, es la denuncia penal. Tratándose de delitos perseguibles a instancia de parte, esto muestra que estos supuestos son percibidos por las propias personas afectadas como más graves[55].

IV. Acceso no autorizado a datos reservados registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo público o privado

SSTS 532/2015, de 23 de septiembre; y sobre todo, 476/2020, de 25 de septiembre (en ambas datos de salud y se aplica el 197.2 y no el tipo agravado. Se reduce el 197.2 a datos relativos al núcleo duro de la intimidad;

STS 412/2020, de 20 de julio, distingue entre quien está legitimado y se extralimita en sus funciones, y quien no está autorizado.

[55] Véanse, entre otras, la SAP Barcelona, 121/2019, de 7 de febrero; SAP Jaén, 432/2017, de 22 de noviembre; SAP Islas Baleares, 197/2017, de 31 de julio; SAP Barcelona, 302/2017, de 24 de abril; SAP Valencia, 488/2016, de 25 de noviembre; SAP Cádiz, 35/2020, de 28 de enero; SAP Madrid, 772/2019, de 2 de diciembre; SAP Navarra, 165/2018, de 26 de junio; SAP Barcelona, 962/2019, de 19 de noviembre; SAP Córdoba, 507/2019, de 12 de noviembre; SAP Asturias, 125/2019, de 28 de marzo; SAP Vizcaya, 90063/2019, de 15 de febrero; SAP Almería, 76/2018, de 14 de febrero; SAP 805/2017, de 20 de diciembre; SAP Madrid, 657/2017, de 15 de noviembre; SAP Madrid, 580/2018, de 25 de septiembre; SAP Santa Cruz de Tenerife, 166/2018, de 16 de mayo; SAP Barcelona, 95/2018, de 23 de febrero. En algunas de estas resoluciones no se aprecia el delito debido a que los hechos tuvieron lugar con anterioridad a la entrada en vigor de la LO 1/2015; a pesar de ello los afectados optaron por interponer denuncia penal.

Derechos laborales y retos de protección social en el trabajo a distancia.

David Montoya Medina
Profesor Titular de Universidad
Universidad de Alicante

1.- Introducción.

El objeto del presente estudio es el de ofrecer una radiografía lo más pegada al terreno posible de los principales problemas de índole jurídico laboral y de protección social que plantea el RDL 28/2020, de 22 de septiembre, *de trabajo a distancia*, norma que entró en vigor el pasado 13 de octubre.

Se trata de una norma importante singularmente por dos razones:

1.- Ha nacido de la concertación social, esto es, constituye el resultado de un proceso de negociación, culminado en acuerdo, entre los sindicatos UGT, CCOO, y las patronales CEOE y CEPYME, lo cual es positivo.

2.- Es una norma pionera en España ya que dota por primera vez en nuestro país a esta particular modalidad de prestación de trabajo de un marco jurídico desarrollado, estable y unitario.

Ello no obstante, la técnica legislativa y sistemática utilizada por el legislador deja mucho que desear pues el RDL 28/2020 no deja de ser una mazamorra de disposiciones de diferente naturaleza y origen. Por un lado, el RDL introduce diversas medidas laborales que no tienen nada que ver con el trabajo a distancia[1]. Por otro, regula multitud de cuestiones de carácter no laboral sino fiscal y administrativo[2].

2.- El porqué del RDL 28/2020: ¿Era necesaria la regulación urgente del trabajo a distancia en España?

La respuesta, a mi juicio, es un sí rotundo que se explica, como es imaginable, por los profundos cambios que ha traído consigo la crisis sanitaria del Covid-19.

España, con ocasión de dicha crisis sanitaria ha sufrido una verdadera catarsis en materia de trabajo a distancia. Hasta hace apenas un año, las estadísticas reflejaban una presencia prácticamente testimonial de esta modalidad de trabajo en nuestro país: solamente un 7,5 % de los asalariados trabajaban en régimen de teletrabajo en comparación con otros países europeos como Países Bajos, Suecia, Finlandia o Dinamarca donde la cifra se ha venido situando en torno al 30-36%.

Ahora, entrados ya en 2020, en apenas unos pocos meses desde que se declaró el estado de alarma, la implantación del trabajo a distancia ha experimentado un golpe de timón pues ha crecido de forma

[1] Como considerar accidente de trabajo los daños a la salud sufridos por personal de centros sanitarios, como consecuencia de haber contraído el Covid-19 en el ejercicio de su trabajo o la simplificación de los trámites para solicitar el ingreso mínimo vital.

[2] Como el tipo impositivo aplicable al IVA de bienes para combatir el COVID-19; modificaciones de la Ley de firma electrónica, de la Ley del juego y la Ley del sector ferroviario. Incluso regula el régimen fiscal aplicable a la final de la "*UEFA Women's Champions League 2020*".

exponencial pillándonos a todos (empresarios, trabajadores, agentes sociales, operadores jurídicos) con el pie cambiado.

1.- Durante los meses iniciales de confinamiento tras la declaración del estado de alarma (marzo y abril), el trabajo a distancia subió hasta una horquilla comprendida entre el 22,3 y el 34%, situándonos al nivel de otros países europeos.

2.- Acabado el confinamiento, conforme a los datos del INE del tercer trimestre del año (julio a septiembre), los trabajadores a distancia representan el 16,2% de los asalariados. Este último dato confirma algo que se dice mucho pero que está por ver: que el teletrabajo ha venido para quedarse.

3.- Aclaraciones conceptuales: trabajo a distancia, teletrabajo, trabajo a domicilio: ¿son conceptos equivalentes?

Trabajo a domicilio, trabajo a distancia y teletrabajo son conceptos próximos que tienden a identificarse, así que conviene distinguirlos.

Trabajo a domicilio y trabajo a distancia son, en realidad, las dos caras de la misma moneda. Tanto el art. 13 del ET de 1980 como el vigente art. 2 del RDL 28/2020 los definen en términos prácticamente análogos como aquella modalidad de la prestación de trabajo que se desarrolla en el domicilio del trabajador o en el lugar libremente elegido por éste. La diferencia es fundamentalmente histórica y tecnológica. El concepto de trabajo a domicilio es más propio de otra época pues, a diferencia del trabajo a distancia, no fue diseñado pensando en que la prestación de trabajo pudiera ser desarrollada de forma remota a través de dispositivos informáticos, telemáticos y de telecomunicación.

Precisamente, el teletrabajo es una modalidad de trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de dispositivos informáticos, telemáticos y de telecomunicación (art. 2 c)

RDL 28/2020). Se caracteriza por tres elementos: 1.- Locativo: el trabajo se desarrolla fuera del centro de trabajo, en el domicilio del trabajador o en cualquier otro lugar. 2.- Instrumental: la utilización de dispositivos informáticos, telemáticos y de telecomunicación para el desarrollo del trabajo. 3.- Temporal: la preponderancia y habitualidad de la prestación de servicios en régimen de teletrabajo.

4.- Antecedentes normativos del trabajo a distancia.

1.- En el plano internacional, todavía está en vigor el Convenio nº 177 de la OIT, de 1996, *sobre trabajo a domicilio*. Se trata de una norma de mínimos cuya finalidad fundamental es garantizar la igualdad de trato entre los trabajadores a domicilio y los trabajadores presenciales.

Dentro de la Unión Europea, existe un *Acuerdo Marco Europeo sobre Teletrabajo*, que fue suscrito por los agentes sociales europeos el 16 de julio de 2002. Si bien dicho texto ha venido reconociendo determinados derechos y garantías concernientes al teletrabajo, no se trataba en puridad de una norma jurídica. Se trata de un acuerdo entre los agentes sociales europeos que reviste eficacia obligacional para sus sujetos firmantes pero carece de efectos vinculantes frente a terceros ya que se limita a introducir directrices para la negociación colectiva nacional. Con todo, es evidente que su contenido ha inspirados al legislador nacional a la hora de regular el trabajo a distancia.

2.- En el marco nacional, el art. 13 ET, desde su versión inicial de 1980, venía regulando el denominado trabajo a domicilio. La reforma laboral de 2012, modificó dicho precepto para reemplazar el viejo concepto de trabajo a domicilio por el más moderno de trabajo a distancia. con el propósito (declarado por la propia exposición de motivos de la Ley 3/2012), de dar expresa cabida al teletrabajo, esto es, al trabajo a distancia basado en el uso intensivo de las nuevas tecnologías.

El nuevo art. 13 ET, sin embargo, venía siendo una norma totalmente anodina, como lo fue su versión de 1980, por la escasa implantación del trabajo a distancia en nuestro país, hasta la llegada de la pandemia.

2.1.- Poco después de la declaración del estado de alarma, el gobierno aprobó el RDL 8/2020, de 17 de marzo[3], cuyo art. 5 introdujo dos medidas claramente dirigidas en este sentido en relación con el denominado trabajo a distancia.

1.- Por una parte, para garantizar el mantenimiento de la actividad empresarial, declaró el carácter preferente del trabajo a distancia exigiendo a las empresas su implantación cuando fuese técnica y razonablemente posible, como mecanismo alternativo a las suspensiones y reducciones de jornada por fuerza mayor. La norma pretendía, pues, servirse del trabajo a distancia para cumplir una triple función: preservar la salud pública, mantener el empleo y favorecer la conciliación de la vida laboral y familiar.

2.- Por otra, con el objeto de facilitar la implementación del trabajo a distancia en aquellas empresas en las que no estuviera prevista hasta el momento, dispuso una relajación de la obligación empresarial de evaluación de los riesgos laborales (art. 16 LPRL), estableciendo que la misma se entendería cumplida, con carácter excepcional, a través de una autoevaluación realizada voluntariamente por la propia persona trabajadora[4].

[3] RDL 8/2020, de 17 de marzo, *de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19*.

[4] Estas medidas fueron diseñadas para durar hasta el mes siguiente a la finalización del estado de alarma con lo cual debieron expirar el 21 de julio. Sin embargo, fueron prorrogadas por dos meses más (art. 15 del RDL 15/2020, de 21 de abril), así que expiraron el pasado 21 de septiembre, víspera precisamente de

5.- El ámbito de aplicación del RDL 28/2020.

El RDL 28/2020 es aplicable no solamente al teletrabajo sino a toda fórmula de trabajo a distancia. Por tanto, aunque no constituye su núcleo principal de imputación normativa, también se aplica al trabajo a domicilio clásico que no constituye teletrabajo.

5.1.- El teletrabajo como principal núcleo de imputación normativa del RDL 28/2020?

El RDL 28/2020 se aplica al teletrabajo como paradigma del trabajo a distancia pero no a cualquier tipo de teletrabajo.

1.- Solamente se aplica al teletrabajo por cuenta ajena pues, como es sabido, el trabajo por cuenta propia se sitúa extramuros de las normas laborales. Ahora bien, cuestión distinta es que el desarrollo de las nuevas tecnologías termine propiciando el teletrabajo por cuenta propia, relegando el prestado por cuenta ajena. En mi opinión, dicha tendencia puede llegar a materializarse en el futuro pues antes de la pandemia el teletrabajo por cuenta propia predominaba claramente frente al prestado por cuenta ajena, por lo que es previsible que cuando la situación sanitaria se normalice, dicha tendencia se acentúe.

2.- Solamente se aplica al teletrabajo por cuenta ajena a domicilio y el teletrabajo móvil o itinerante (ej. personal de mantenimiento de equipos informáticos). Por tanto, no se aplica al teletrabajo en telecentros, esto es, el desarrollado en centros de trabajo pertenecientes a la empresa o a terceros (ej. teleoperadores en "*Call Centres*"). Téngase en cuenta que dicha modalidad de teletrabajo, al no desarrollarse en el lugar libremente elegido por el trabajador, no es técnicamente trabajo a distancia por más que implique la utilización de equipos informáticos o

la aprobación de la norma actualmente en vigor: el RDL 28/2020, de 22 de septiembre, de trabajo a distancia.

telemáticos. Este tipo de teletrabajo se somete, pues, a la normativa laboral común.

3.- Se aplica solamente al teletrabajo desarrollado "*con carácter regular*". La norma especifica que el teletrabajo es regular si se presta durante al menos el 30% de la jornada en un periodo de referencia de 3 meses o el porcentaje proporcional equivalente en función de la duración del contrato. Sobre el particular cabe decir lo siguiente:

- El periodo de referencia de 3 meses se introduce pensando en los teletrabajadores que no todos los días o no todas las semanas prestan servicios en régimen de teletrabajo.

- El porcentaje se debe reducir proporcionalmente cuando se trate de trabajadores temporales con un contrato de duración inferior a 3 meses (Ej. Trabajador con contrato temporal de mes y medio será teletrabajador si un 15% de su jornada se desarrolla en régimen de teletrabajo).

- Cuando se trata de trabajadores menores de edad y trabajadores con contratos formativos (prácticas y para la formación) la norma exige un porcentaje de presencialidad no inferior al 50%.

4.- El RDL no se aplica al teletrabajo en la Administración Pública. La norma establece que al mismo será aplicable una normativa específica y, mientras ésta no sea aprobada, sus teletrabajadores se regirán por el art. 13 ET en su redacción anterior al RDL 28/2020 (Disp. Adic. 2ª y Disp. Transit. 2ª).

6.- Presupuestos definidores del régimen jurídico del trabajo a distancia.

Las principales notas características del trabajo a distancia regulador por el RDL 28/2020 son la voluntariedad en la prestación de

servicios a distancia, su reversibilidad y el régimen de preferencias previsto en la norma.

6.1.- La voluntariedad del trabajo a distancia.

El RDL 28/2020 exige que la prestación de servicios a distancia sea voluntaria. Por tanto, no puede ser impuesta por el empresario ni siquiera en el ejercicio de su poder de modificación sustancial de condiciones de trabajo del art. 41 ET (art. 5.1 RDL 28/2020). Se trata de una regla prácticamente análoga a la existente para el trabajo a tiempo parcial.

La norma refuerza la garantía de la voluntariedad disponiendo que la negativa del trabajador a trabajar a distancia no podrá comportar la válida extinción del contrato de trabajo ni una modificación sustancial de condiciones. Incluso se prohíbe el despido y la modificación sustancial cuando el trabajador acepte pasar a prestar servicios a distancia pero evidencie dificultades para el desarrollo adecuado de su actividad.

El cumplimiento del presupuesto de la voluntariedad se plasma con la firma del denominado *Acuerdo de Trabajo a Distancia*. Se trata de un acuerdo individual, que debe ser concertado por escrito, y que permite constatar el consentimiento de las partes. El acuerdo puede formar parte del contrato de trabajo inicial o incorporarse posteriormente. En todo caso, debe formalizarse antes de que se inicie el trabajo a distancia.

El acuerdo de trabajo a distancia tiene un contenido mínimo fijado por el art. 7 RDL 28/2020 que puede ser complementado por la negociación colectiva. Entre dicho contenido figuran extremos tales como un inventario de los equipos y muebles necesarios para el desarrollo del trabajo a distancia, los gastos del trabajador asociados a la prestación de trabajo y la fórmula para su compensación, el horario de trabajo, el porcentaje de distribución entre presencialidad y trabajo a distancia, el

lugar elegido por el trabajador para la prestación de trabajo, el centro de trabajo al que se adscribe el trabajador, la duración del acuerdo, etc.

6.2.- La reversibilidad del trabajo a distancia.

Junto a la voluntariedad, el art. 5 RDL 28/2020 dispone que en el supuesto de que el trabajador preste inicialmente servicios con carácter presencial y pase voluntariamente a trabajar a distancia, dicha decisión será reversible para el mismo y para la empresa. Se trata, pues, de una suerte de derecho de retractación que puede ejercitar cualquier de las partes y que rige solamente en caso de transición de trabajo presencial a trabajo a distancia (no viceversa).

Se trata, no obstante, de un derecho carente de desarrollo pues la norma remite los términos de su ejercicio (causas y procedimiento) a la negociación colectiva y, en su defecto, al acuerdo de trabajo a distancia. Queda pues la duda de si se puede reconocer este derecho en caso de que la negociación colectiva no diga nada. A mi juicio, todo hace pensar que sí, siendo suficiente respetar un plazo de preaviso para la retractación ya que uno de los contenidos mínimos del acuerdo de trabajo a distancia es dicho plazo de preaviso.

La norma establece como garantía del derecho a la reversibilidad que su ejercicio no pueda ser causa de extinción de la relación laboral ni de modificación sustancial.

6.3.- El régimen de preferencias.

Junto a la reversibilidad, el art. 8 RDL 28/2020 llama a la negociación colectiva para regular preferencias para pasar de trabajo presencial a distancia y viceversa, sugiriendo diversas causas para ello: razones formativas, de mantenimiento en el empleo de personas con

diversidad funcional o sensibles a determinados riesgos, pluriempleo del trabajador o por sus circunstancias personales y familiares.

Aparte de ello, la norma reconoce preferencia para ocupar puestos de trabajo presenciales a aquellos trabajadores que desde el inicio de su relación laboral realizan trabajo a distancia durante la totalidad de su jornada de trabajo. Dicha preferencia, unida a la reversibilidad de la decisión de trabajar a distancia, revela un claro recelo del legislador hacia esta modalidad de trabajo.

7.- Derechos reconocidos por el RDL 28/2020 a los trabajadores a distancia.

Dichos derechos se reconocen en los arts. 9 y siguientes. De entre ellos, me voy a referir solamente a aquellos que revisten mayor interés bien por tener un alcance difuso, bien por ser susceptibles de plantear más problemas jurídicos y, por tanto, una mayor litigiosidad.

7.1- Derechos relacionados con los equipos de trabajo y los gastos de la actividad laboral.

La norma reconoce, por una parte, el derecho de los trabajadores a distancia a la dotación y mantenimiento adecuado de todos los medios y equipos necesarios para el desarrollo de su actividad (art. 11 RDL 28/2020).

Por otra parte, reconoce el derecho a que los gastos generados por el desarrollo de la actividad laboral sean sufragados o compensados por la empresa en la forma que establezca el convenio colectivo (art. 12 RDL 28/2020). Caben, por tanto, dos sistemas: bien que la empresa asuma directamente dicho coste, bien que lo asuma el trabajador pero que se lo compense la empresa en los términos previstos en el convenio colectivo.

Dicha regulación, que se discutió mucho en las fases previas de elaboración de la norma, va a ser muy útil para deslindar el teletrabajo

por cuenta ajena del prestado por cuenta propia pues si el coste de los equipos y medios, de su mantenimiento y de los gastos ocasionados durante la ejecución de la actividad laboral es asumido por la empresa es evidente que existe ajenidad y, por tanto, relación laboral.

7.2.- Derechos relacionados con el tiempo de trabajo.

En relación con el tiempo de trabajo, el RDL 28/2020 reconoce el derecho al horario flexible (art. 13), el derecho al control horario (arts. 7 c) y 14) y el derecho a la desconexión digital (art. 18).

El derecho a la flexibilidad horaria resulta, en cierto modo, redundante, pues parece que dicha característica es inherente al trabajo a distancia. Difícil es concebir el trabajo a distancia sin flexibilidad horaria.

Por su parte, los derechos al control horario y a la desconexión digital han sido instaurados para combatir uno de los problemas típicos asociados al trabajo a distancia: la prolongación excesiva de la jornada tanto a instancia del empresario como del propio trabajador.

Con respecto al control horario, el RDL 28/2020 impone que el horario del teletrabajador se refleje en el acuerdo de trabajo a distancia y que el registro empresarial del mismo al que ya obliga nuestra legislación para todo trabajador[5], se efectúe de tal forma que refleje fielmente el tiempo que el teletrabajador dedica a la prestación laboral. Esto último es importante porque implica que, en la práctica, no será suficiente con registrar la hora de comienzo y de finalización de la jornada diaria. También habrá que registrar el momento de activación y de desactivación

[5] El derecho al registro horario fue introducido en el art. 34 ET por el RDL 8/2019, de 8 de marzo, con el objeto de combatir las horas extra no declaradas

de los equipos (lo cual es técnicamente posible) e, incluso, el tiempo de preparación de cada una de las tareas.

En cuanto al derecho a desconexión, a mi juicio, el art. 18 RDL 28/2020 deja bastante que desear pues prácticamente se limita a reproducir la regulación de este derecho en el art. 88 de la Ley Orgánica de Protección de Datos.

Debe advertirse que el derecho de desconexión puede ser muy eficaz cuando los excesos de jornada se produzcan a instancias del empresario pero resultará totalmente inoperativo cuando dichos excesos se produzcan por propia voluntad del trabajador.

Para estos casos, el art. 18 RDL se limita a reiterar la obligación empresarial, prevista en el art. 88 de la Ley Orgánica de Protección de Datos, de elaborar una política interna dirigida a concienciar a los trabajadores sobre un uso razonable de las herramientas tecnológicas para evitar el riesgo de fatiga informática. Aquí echo en falta dos medidas. Por un lado, falta una llamada a la negociación colectiva y al acuerdo individual para el establecimiento obligatorio de sistemas de desactivación de los equipos (*siestas digitales*). Por otro, creo que la norma debería haber dado un espaldarazo al ejercicio del poder disciplinario del empresario en caso de transgresión por el trabajador de los límites de jornada, pues algunas sentencias vienen sosteniendo criterios claramente restrictivos en estos supuestos.

7.3.- Derechos concernientes a la prevención de riesgos laborales.

El art. 15 RDL 28/2020 reconoce a los trabajadores a distancia el derecho a una adecuada protección en materia de seguridad y salud en el trabajo. En el marco de este derecho, la empresa está obligada al cumplimiento de sus obligaciones preventivas de evaluación de riesgos y de planificación de la actividad preventiva.

Cuando el trabajo a distancia se desarrolla en el domicilio del trabajador, el cumplimiento de dichas obligaciones empresariales puede resultar enojosa por cuanto el acceso empresarial al puesto de trabajo se encuentra limitado por la garantía constitucional de la inviolabilidad del domicilio. Igual limitación puede afectar a los delegados de prevención y a la propia Inspección de Trabajo en el ejercicio de sus competencias de vigilancia y control sobre las condiciones de trabajo.

Puede producirse un problema de difícil solución en los casos en que el acceso del empresario al domicilio del trabajador sea necesario para el cumplimiento de sus obligaciones preventivas, éste lo niegue y, sin embargo, permita la visita de la Inspección de Trabajo de cuya actuación se derive un acta de infracción por deficientes condiciones de seguridad y salud del puesto de trabajo.

Creo que este tipo de situaciones extremas (un tanto esperpénticas, pero factibles) pueden evitarse con un adecuado ejercicio de pedagogía de la cultura preventiva en la empresa, respecto de sus trabajadores, a través del reforzamiento de los deberes empresariales de información y formación frente los riesgos laborales. La idea sería la de concienciarles bien sobre la importancia de trabajar en un entorno seguro. El art. 16.2 RDL va en esta línea al exigir la entrega al trabajador y a los delegados de prevención de un informe escrito motivado para que pueda conocer los motivos y finalidad de la visita.

También podrían ir en esta dirección las "*cláusulas de colaboración*", que podrían insertarse en el acuerdo de trabajo a distancia, en virtud de las cuales el trabajador se comprometiese a facilitar a todos los sujetos con potestades en materia preventiva el acceso al puesto de trabajo. Ello no obstante, dichas cláusulas no dejarían de ser un mero desiderátum, sin obligatoriedad alguna, ya que

la inviolabilidad del domicilio constituye un límite infranqueable. Por tanto, nada impediría que el trabajador revocase lícitamente el consentimiento que hubiese podido manifestar en el contrato sin que se le deparase por ello responsabilidad alguna.

En los casos extremos en los que el acceso del empresario al domicilio del trabajador fuese necesario para evaluar los riesgos y éste persistiese en su negativa el art. 16.2 RDL parece claudicar estableciendo que la dicha evaluación se efectúe en función de la información proporcionada por el trabajador que puede, por hipótesis, resultar insuficiente y/o inadecuada. Aquí no hubiese estado de más que el RDL hubiese introducido una cláusula de exoneración de responsabilidad empresarial cuando no se hubiese podido efectuar una adecuada evaluación de los riesgos debido a la nula disposición del trabajador a colaborar para el cumplimiento de este deber empresarial.

8.- Problemas de protección social del trabajo a distancia.

El trabajo a distancia plantea diversos interrogantes en materia de Seguridad Social. De entre ellos, es dable plantearse, por una parte, si si pueden ser calificados como riesgos profesionales los daños a la salud que puede sufrir el teletrabajador en el desempeño de su prestación de trabajo. Por otra, también resulta de interés determinar hasta qué punto las situaciones de accidente in itinere y de accidente en misión, previstas actualmente en nuestro vigente ordenamiento jurídico de Seguridad Social, pueden acaecer en el trabajo a distancia.

El problema está en que en nuestro ordenamiento jurídico rige un sistema de lista cerrada para la determinación de las enfermedades profesionales de tal forma que solo se pueden calificar como tales aquellas previstas reglamentariamente y por la acción de elementos o sustancias también normativamente previstas (art. 157 LGSS).

Pues bien, cuando uno va al vigente cuadro de enfermedades profesionales (RD 1299/2006) y busca alguna que pueda asociarse al teletrabajo la única que encuentra es el "*síndrome del túnel carpiano*". En otras palabras, no están contemplados ni uno solo de los riesgos psicosociales típicos del teletrabajo: fatiga informática (visual, mental, corporal), tecnoestrés, tecnoadicciones, ciberacoso, etc).

Por ese motivo, hoy por hoy, la única vía que ofrece nuestro ordenamiento jurídico para la calificación de dichas lesiones a la salud como contingencias profesionales es reconducirlas al concepto de accidente de trabajo ya que nuestra legislación conceptúa como accidentes de trabajo las denominadas "*enfermedades del trabajo*", esto es, aquellas dolencias que contraiga el trabajador con motivo de la prestación de trabajo (art. 156.2 e) LGSS).

Esta reconducción, sin embargo, es problemática por dos razones. En primer lugar, porque, conforme a nuestra legislación, el trabajador tiene la carga de demostrar que la enfermedad tuvo "*por causa exclusiva*" la ejecución del trabajo, lo cual es particularmente difícil tratándose de dolencias de origen psicosocial y mucho más si se trata de un teletrabajador que trabaja en su casa. En segundo lugar, porque, si bien nuestra legislación califica como accidente de trabajo, las lesiones que sufra el trabajador durante el tiempo y en el lugar de trabajo, salvo prueba en contrario (art. 156.3 LGSS), dicha presunción produce fricciones cuando se pretende aplicar al teletrabajo ya que fue construida en los años 60 y, por tanto, diseñada pensando exclusivamente en una relación de trabajo presencial. Por tanto, no parece resultar del todo operativa para el trabajo a distancia.

Pero no sólo es eso. La aplicación sin más de la presunción de existencia de accidente de trabajo puede comportar efectos indeseados:

conlleva el riesgo de amparar el fraude del teletrabajador calificando como accidentes de trabajo lo que no son sino puros accidentes domésticos. Tal vez para los supuestos de teletrabajo tendría más sentido aplicar la presunción en sentido inverso, esto es, considerar que la lesión sufrida por el trabajador durante el tiempo y el lugar de trabajo no es accidente de trabajo salvo prueba en contrario.

En cualquier caso, la presente problemática pone en evidencia la imperiosa necesidad de una nueva intervención del legislador para, por un lado, actualizar el cuadro de enfermedades profesionales para dar cabida a las derivadas de los riesgos psicosociales y, por otro, introducir una regulación legal *ad hoc* del accidente de trabajo en el teletrabajo que permita deslindarlo nítidamente del accidente doméstico.

Otra cuestión es la de si en el trabajo a distancia tiene cabida o no el denominado *accidente in itinere* y el llamado *accidente en misión*.

Respecto al *accidente in itinere* es evidente que están claramente expuestos al mismo tanto los trabajadores que realizan teletrabajo móvil o itinerante como los trabajadores a domicilio que realizan parte de su jornada de forma presencial en el centro de trabajo. Los trabajadores que desempeñan la totalidad de su jornada en su domicilio tampoco resultan totalmente inmunes al *accidente in itinere* pues nuestra jurisprudencia ha dicho que procede calificar como tal el sufrido durante el desplazamiento de una segunda residencia al domicilio habitual para incorporarse al trabajo.

Con respecto al *accidente en misión*, esto es, el sufrido con ocasión de tareas realizadas espontáneamente por el trabajador en interés de la empresa, también son imaginables diversos supuestos con el trabajador a domicilio como protagonista. Basta pensar en el que pudiera sufrir al desplazarse puntualmente al centro de trabajo para un curso de

formación, una reunión con otros trabajadores o un reconocimiento médico. También el que pudiera sufrir al desplazarse a un comercio para adquirir material informático. Incluso el sufrido en su propio domicilio cuando accede a dependencias distintas de su puesto de trabajo (garaje, trastero, desván) pero con motivo de la prestación de trabajo.

INFORME DE ACTIVIDADES PARA PROYECTO

"COLOQUIO DE ÉTICA DIGITAL"

El presente informe da cuenta de las recientes actividades relacionadas al proyecto para realizar el evento "Coloquio de Ética Digital", coorganizado por el Departamento de Filosofía del Derecho y Derecho Internacional Privado de la Universidad de Alicante y el Proyecto CENID (Centro de Inteligencia Digital) de la Provincia de Alicante.

1. OBJETIVOS

1.1. Objetivo general

Realizar un evento de transferencia de conocimiento al gran público, en torno a los crecientes desafíos que supone el medio digital para la reflexión ética, tanto para el razonamiento moral intuitivo como para el razonamiento moral crítico. Dicho evento está previsto para mediados de enero de 2021 en la ciudad de Alicante. El mismo busca contar con especialistas de distintas disciplinas que, de modo mixto (asíncrono y síncrono), ofrezcan su perspectiva crítica en torno a los temas más acuciantes que la ética digital supone para el presente y el futuro reciente de nuestras prácticas sociales.

1.2. Objetivos específicos

- Seleccionar los perfiles de los investigadores que participarán de modo asíncrono mediante vídeos breves (alrededor de quince minutos) de acuerdo a los criterios de: a) experiencia y reputación en el campo de estudios, b) diversidad temática y disciplinar y c) paridad de género.
- Enviar invitaciones a los investigadores seleccionados explicándoles las particularidades de la modalidad (el carácter asíncrono) y los lineamientos básicos de la misma (el lenguaje divulgativo, la concisión, la pertinencia temática y el plazo del envío: 25 de noviembre de 2020).
- Visionar los vídeos para comprobar la calidad de sonido y de imagen y el cumplimiento de los lineamientos básicos.
- Revisar críticamente los vídeos, para elaborar una presentación de los mismos en la que se subrayen los puntos salientes en la discusión síncrona a llevar adelante con los Dres. M. Atienza, M. Palomar, N. Oliver y A. Pedreño.

- Transcribir los vídeos en lengua extranjera para su traducción y añadido de subtítulos, en el marco de la post-edición de los mismos en la cual también se incluirán logos institucionales e imágenes, que sirvan de apoyo para la mejor comprensión de los vídeos de los especialistas.
- Elaborar un breve libro que oficie de actas del evento y que permita a los participantes ampliar su contribución para que quede constancia escrita de su aporte.

2. ACTIVIDADES REALIZADAS

En una primera etapa se seleccionaron los perfiles de acuerdo a recomendaciones de colegas del ámbito de la ética y a una breve investigación de los perfiles asociados a términos como "ética digital", "ética de la información" y "ciberética" en Google Scholar y otras redes académicas, preseleccionando de acuerdo a los criterios mencionados en los objetivos específicos.

En esa primera etapa se invitó a Mariarosaria Taddeo (miembro del Laboratorio de Ética Digital de la Universidad de Oxford, Gran Bretaña), Primavera De Filippi (Investigadora permanente del CNRS, París, y miembro del Berkman Center de la Universidad de Harvard), Javier Echeverría (miembro de Jakiunde, España), Maxime Lambrecht (Universidad Católica de Lovaina, Bélgica), Pablo Lapostol (miembro del grupo de investigación GobLab de la Universidad Adolfo Ibáñez, Chile), Dolores Sánchez Almendros (miembro del Centro Superior de Investigaciones Científicas, España).

El Dr. Lambrecht y la Dra. Taddeo, que habían aceptado participar enviando su vídeo, debieron excusar su participación a último momento debido a razones personales y de salud respectivamente. Por lo cual, hubo que hacer algunos ajustes en el programa y en el presupuesto presentado en el informe anterior (el del 9 de noviembre de 2020). En cuanto al programa, el mismo se redujo a cinco expositores y se le pidió a la investigadora Dolores Sánchez Almendros que ofreciera una perspectiva crítica de la "ética de la información" de acuerdo a la visión predominante en el *Digital Ethics Lab* de Oxford, que inicialmente expondría la Dra. Taddeo. Al tiempo que se complementará el vídeo faltante con otro de Lucas Misseri que oficie de estado de la cuestión. Resultando el programa definitivo del siguiente modo:

1. **Lucas E. Misseri** (profesor visitante en UA, España), presentando un vídeo introductorio "Ética digital: estado de la cuestión".
2. **Javier Echeverría** (miembro de Jakiunde, España), presentando su contribución titulada: "La ampliación de los Derechos Humanos al entorno digital".

3. **Dolores Sánchez Almendros** (miembro del Centro Superior de Investigaciones Científicas, España), dando cuenta críticamente de la visión oxoniense en su ponencia "La ética de la información en la perspectiva de L. Floridi".
4. **Juan Pablo Lapostol** (miembro del grupo de investigación GobLab de la Universidad Adolfo Ibáñez, Chile), exponiendo su trabajo: "Inteligencia artificial y creación de Derecho".
5. **Primavera De Filippi** (Investigadora permanente del CNRS, París, y miembro del Berkman Center de la Universidad de Harvard) cerrando con su trabajo: "Blockchain Technology and the Rule of Code: Regulation via Governance" [Tecnología blockchain y el imperio del código: regulación por medio de la gobernanza].

Posteriormente con la ayuda de la coordinadora del rectorado, María Juana Marco Marco, se medió para dar de alta a los participantes del evento como proveedores para la Universidad de Alicante. Los investigadores fueron asistidos en el proceso de rellenado del formulario y en la recolección de datos personales, siempre respetando la normativa de protección de datos vigente. Por las diferencias entre los sistemas fiscales y bancarios de los diversos países de origen de los investigadores (Francia y Chile) hubo algunos inconvenientes, pero los mismos fueron solucionados.

Asimismo, se mantuvo una comunicación continua entre los investigadores y Lucas Misseri para asistirlos en el proceso de grabación de sus correspondientes contribuciones asíncronas. Ayudándolos a seleccionar adecuadamente el tema de acuerdo al auditorio, recordándoles las pautas de extensión, verificando el cumplimiento de ciertos estándares de calidad audiovisual y sugiriendo revisiones en caso de que fuera necesario. En este sentido Almendros envió dos versiones de su vídeo, para mejorar la calidad de sonido. Por último, se los asistió en el alta de los vídeos a la nube y los mismos fueron alojados en una cuenta GCloud de la Universidad de Alicante en los siguientes enlaces:

- Contribución de Almendros: https://drive.google.com/file/d/18GXc_alXwd3m94CjxfOEkU4_F0HRbyUQ/view?usp=sharing
- Contribución de De Filippi: https://drive.google.com/file/d/131j5BVM5bsF3Wuy9KtVWgWYtrSkmkxq8/view?usp=sharing
- Contribución de Echeverría: https://drive.google.com/file/d/12fi-4CAePlNHpSfeRtRmN4W8x5bEZZ2V/view?usp=sharing

- Contribución de Lapostol: https://drive.google.com/file/d/10vBkwXqQbbk4Q0eJFvEQWkFOJn17lxf9/view?usp=sharing

San Vicente del Raspeig, 27 de noviembre de 2020