CAPÍTULO III
INCIDENCIA DE LA INTELIGENCIA ARTIFICIAL EN LOS DERECHOS FUNDAMENTALES

1. Cuestiones previas

Parece claro que no se puede aspirar a crear un nuevo derecho fundamental como consecuencia del surgimiento de cada una de las nuevas posibilidades tecnológicas, dado que no todas tienen el mismo grado de incidencia en las concepciones jurídicas, y no todas tienen la misma transcendencia desde la perspectiva jurídica. Incluso los denominados por la LO 3/2018, y de forma algo pretenciosa, derechos digitales, en su mayoría son concreciones o variantes aplicativas de los derechos fundamentales ya reconocidos en nuestro ordenamiento jurídico y el europeo, y suficientemente garantizados. Ningún ordenamiento jurídico puede pretender dar respuesta concreta a cada una de las posibilidades de vulneración o intromisión en los derechos fundamentales. La técnica aplicada hasta ahora ha sido, a través de la legislación y la jurisprudencia, ir adecuando los derechos existentes a las nuevas vulneraciones, ir ampliando las interpretaciones y solventando las omisiones, a la vez que formulando tendencias interpretativas, que con el tiempo tienen su plasmación en nuevas normativas.

La STC 58/2018 es muy clarificadora a este respecto, y de forma concreta manifiesta que "… Los avances tecnológicos y el fenómeno de la globalización a través de internet y de otras vías dan lugar a nuevas realidades que, de una u otra forma, pueden incidir sobre el ejercicio de los derechos fundamentales, su delimitación y su protección, lo que obliga a este Tribunal a una constante labor de actualización de su doctrina para adecuarla a la cambiante realidad social, con el fin de dar una respuesta constitucional a esas nuevas situaciones…"[25]. De igual forma, la jurisprudencia habrá de ir tejiendo la argumentación y fundamentación de variaciones en los derechos, armando una estructura lógico-jurídica de los derechos fundamentales, que

[25] STC 58/2018, de 4 de junio, f. j. 4.

produzca una respuesta adecuada a las nuevas necesidades jurídicas y que palié las deficiencias normativas, a la vez que facilite su aplicabilidad y ejecución material. La protección jurídica y los medios de garantía ya existen, lo que varían son las formas de vulneración, por ello no es necesario crear un ordenamiento jurídico *ex novo*, es necesario ir adecuando el existente a las nuevas necesidades, y ello es tarea tanto del legislador, de la jurisprudencia, y también de la doctrina.

Parece claro, que la nueva sociedad digital no puede ser ahormada únicamente por el Derecho, teniendo en cuenta que supone una nueva conformación horizontal del conjunto social, y que afecta a los medios de comunicación, a la economía, a todos los ámbitos de lo social, incluso a las mismas bases de organización social y política. Por ello parece muy acertada la propuesta de De la Quadra Salcedo, cuando usa el concepto de la solución holística[26], y de forma concreta manifiesta que "Esa afección a todos los elementos fundamentales que estructuran e informan nuestras sociedades hace obligatorio adoptar una perspectiva holística en el tratamiento de los retos que plantea la sociedad digital"[27]. Atribuir al Derecho la única forma de ordenar y encajar la sociedad digital es un grave error. El Derecho debe ser, como ha sido siempre, una forma de solventar conflictos sociales con una perspectiva de bien común, pero en todo caso necesita de la colaboración de otras áreas de conocimiento, de todos los elementos que conforman la estructuración social.

Las soluciones aportadas por el Derecho hasta ahora parecen de todo punto insuficientes. Hacemos repaso de estas. El Derecho internacional tiene una limitada capacidad coactiva, por su escasa vinculación y su menor entidad sancionadora. Su efectividad se limita a áreas muy concretas, como es el comercio a nivel mundial, algunos aspectos de propiedad intelectual y quizás con mayor eficacia, en materia de elaboración de tratados.

Otro ámbito en que de alguna forma se viene regulando la sociedad digital es el Derecho de defensa de la competencia. Las regulaciones nacionales encuentran grandes dificultades a la hora de la normación por la presión que ejercen de forma genérica las grandes empresas de tecnología, dado que aquélla siempre limita su capacidad de maniobra, a la vez que tienen múltiples formas de ir eludiendo las regulaciones nacionales. De igual manera, evitan con facilidad la competencia entre ellas, de tal manera que las denominadas "cinco grandes" (Google, Facebook, Microsoft, Amazon y Appel) se quedan con todo el mercado.

La única herramienta de control sobre las empresas tecnológicas hasta la fecha ha venido a través del derecho de la libre competencia. De esta forma,

---

[26] Entendida en su formulación aristotélica como "el todo es mayor que la suma de sus partes".

[27] DE LA QUADRA SALCEDO FERNÁRDEZ DEL CASTILLO, T: *Retos, riesgos y oportunidades de la sociedad digital*, en la obra de VV. AA. *Sociedad Digital y Derecho*. BOE. Madrid 2018, pág. 63.

tanto algunos Estados europeos, como la propia Unión Europea, han impuesto sanciones económicas a algunas de ellas, pero que han sido asumidas más como un coste añadido de producción, que como reproche jurídico efectivo a su actividad o a la forma de llevarla a efecto. En todo caso, y como nos recuerda Hoffmann-Riem, el derecho de defensa de la competencia tiene como finalidad "garantizar la funcionalidad de los mercados económicos y para impedir el abuso de una posición de dominio de mercado … pero no es un Derecho específico para limitar otros poderes (por ejemplo, políticos, culturales, sociales o de otra índole). El logro de objetivos de bien común como la protección de la autonomía (libertad frente a la manipulación), la equidad de oportunidades de acceso, la supresión de la discriminación o la formación de una opinión pública dirigida a la reproducción y promoción de la pluralidad social, no son objetivo específico del Derecho de defensa de la competencia"[28].

Parece adecuado deducir que las soluciones que tiene que aportar el Derecho han de venir de la extensión aplicativa de principios jurídicos a las nuevas necesidades sociales. Como nos recordara García de Enterría, "la ciencia jurídica no tiene otra misión que la de desvelar y descubrir a través de conexiones de sentido cada vez más profundas y ricas, mediante la construcción de instituciones y la integración respectiva de todas ellas en un conjunto, los principios generales sobre los que se articula y debe, por consiguiente, expresarse el orden jurídico. Este, en la sugerente expresión de SIMONIUS, «está impregnado de principios hasta sus últimas ramificaciones», de modo que en hacer patente esa oculta y profunda vida de los principios está la augusta función del científico del Derecho, y no en ofrecer clasificaciones o sistematizaciones geométricas, lógicas o nemotécnicas de la materia de las leyes. Una ciencia jurídica puramente exegética (aunque quisiese incluir los «principios incluidos por el legislador en sus normas») no podría responder nunca a la clásica objeción de VON KIRCHMANN : «tres palabras rectificadoras del legislador convierten bibliotecas enteras en basura»; el que esto no haya sido así y las obras de los grandes juristas de la historia no sólo no sean basura, sino que hayan adquirido un permanente y eficaz valor clásico, es justamente porque en ellas se ha acertado a expresar un orden institucional de principios jurídicos no sometidos a la usura del tiempo. La superioridad del Derecho Romano sobre otros sistemas jurídicos históricos anteriores o posteriores estuvo justamente, no ya en la mayor perfección de sus leyes … sino en que sus juristas fueron los primeros que se adentraron en una jurisprudencia según principios, la cual ha acreditado su fecundidad, e incluso, paradójicamente, su perennidad, y hasta su superior certeza, frente a cualquier código perfecto y cerrado de todos los que la historia nos presenta"[29].

---

[28] Obra citada, páginas 102 y 103.

[29] GARCÍA DE ENTERRÍA, E: *Reflexiones sobre la Ley y los principios generales del Derecho Administrativo*. Texto extraido de https://dialnet.unirioja.es, páginas 201 y 202.

La aportación que el jurista puede realizar a esta novedosa realidad social que denominamos sociedad digital, ha de venir, inexorablemente, precedida del entendimiento del bagaje jurídico, que ha de cohonestarse con las nuevas necesidades. Ello ha de llevarse a efecto en base a la reconfiguración de principios jurídicos que nacen de una pretensión de ordenación social heredada, a la que se deben sumar las nuevas necesidades.

Pero este proceso no puede realizarse sin contextualización, ni ser el producto de un laboratorio aislado o desconocedor de las realidades sociales. Es una tarea de conjunto, y no menor. En definitiva, se trata de ir incardinando, a la vez que adecuando, el ordenamiento jurídico a las nuevas necesidades sociales. Para ello, es necesario el análisis concreto de los puntos jurídicos de mayor fricción o de superior dificultad de encaje, y de forma más concreta, los derechos y libertades fundamentales más expuestos a las innovaciones que provienen o generará el desarrollo de una sociedad digital, y con posterioridad, ir verificando las posibles soluciones jurídicas.

Para delimitar esta pretensión, hemos seleccionado el análisis de aquellos derechos fundamentales que entendemos más expuestos al uso de la IA. De esta forma, los derechos de carácter personal, la libertad ideológica, el derecho a la información y la libertad de expresión, junto con el derecho a la igualdad, se presentan como el núcleo de incidencia y el objeto de soluciones jurídicas. No existe la menor duda de que hay también afectación, directa o indirecta, de otros derechos, pero entendemos que la troncalidad de los referidos en la ordenación social, justifican esta selección del objeto de estudio.

Otro aspecto que conviene concretar antes del análisis específico de los derechos fundamentales es que nos movemos en un contexto de permanente cambio. No ya cada año, sino cada mes, surge una nueva posibilidad, una mejora de aplicabilidad, se repara en una circunstancia que no había sido prevista. Las posibilidades técnicas tienen un crecimiento exponencial en cuanto a su creación y aplicabilidad en el tiempo. Por el contrario, el Derecho, como ya conocemos, es lento en su respuesta, y requiere de la actuación coordinada de muchos operadores (legislador, jurisprudencia, Administraciones Pública, órganos de control, etc.) a lo que se suma la necesidad de actuar también en diversos niveles, como el regional, o internacional. Por muy previsores que sean los ordenamientos jurídicos, la IA tiene un fuerte componente de imprevisibilidad, de resultados o consecuencias colaterales no previstas, y que, en su propia creación y aplicación, requieren de un proceso de control y readaptación permanente. Esto supone una dificultad añadida al Derecho como respuesta, y se constituye en el riego más sustantivo de la IA.

2. Derecho a la intimidad

En 2013 Edward Snowden reveló la existencia de programas promovidos por los Estados Unidos junto con otros países (Canadá, Australia, Gran Bre-

taña y Nueva Zelanda) a través de los que se realizaban actividades de vigilancia y espionaje masivo a nivel mundial. En particular, se trataba de dos programas de vigilancia electrónica confidencial a cargo de la NSA (Agencia de Seguridad Nacional de los Estados Unidos); PRISM, que desde 2007 se utilizó para recabar de manera no consentida información de más de 35 líderes mundiales; y XKeyscore, creado en 2008 para la búsqueda y análisis masivo de datos en internet.

Según las revelaciones de Snowden, en su lucha contra el terrorismo, la NSA utiliza técnicas de espionaje diversas como la introducción de software espía en aplicaciones móviles muy populares como Angry Birds o Google Maps, la ruptura de la seguridad de los sistemas operativos iOS, Android, o la violación de los cifrados de las BlackBerry y teléfonos móviles. Se infectan cientos de miles de redes informáticas con malware a nivel internacional e incluso se espían los correos electrónicos de Hotmail, Outlook o Gmail. Se vigilan y almacenan miles de millones de llamadas y registros telefónicos. De esta manera, se consiguen contactos, datos de geolocalización, fotografías, aplicaciones o mensajes, datos que les permiten crear perfiles de prácticamente cualquier individuo, pues a partir de esto pueden deducir su modo de vida, país de origen, edad, sexo, ingresos, comunicaciones y contenidos de estas, actividades personales y profesionales, y un largo etc.

La empresa israelí NSO ha desarrollado en 2010 el programa Pegasus, que vende, en teoría, únicamente a Estados, y que consiste en un software espía que se introduce en los teléfonos móviles y ofrece un control prácticamente ilimitado de funciones sobre el mismo (accede a la ubicación, graba conversaciones, accede a imágenes o videos y activa sus cámaras en control remoto, accede a correos electrónicos, agendas, etc.). Lo hace durante 24 horas al día y no deja rastro de su presencia. Su finalidad originaria es la prevención del terrorismo y el narcotráfico, si bien los servicios de inteligencia de los distintos países pueden darles el uso que estimen más conveniente, conforme a sus necesidades.

Su uso en España por parte del Gobierno produjo en abril de 2022 una grave crisis política por el supuesto uso en el entorno independentista catalán, que se resolvió con la dimisión de la directora del Centro Nacional de Inteligencia y algunos cambios estructurales relativos a la dependencia y funciones del citado organismo. La relevancia informativa del asunto decayó, la tormenta política se diluyó, y como parece propio, no hubo más debate público al respecto de los programas espía, de su uso, de su control, ni de sus posibilidades, o lo más importante, de la posible afectación a derechos y libertades fundamentales.

Los estudios realizados en el campo de la ciencia social computacional concluyen que se puede conocer la personalidad de un individuo por su forma de expresarse, por sus actuaciones, el carácter de lo que publica, cuánto y con qué frecuencia lo hace, o por su forma de interactuar, entre otras infi-

nitas opciones. Todo este rastro o huella digital dan lugar a la configuración de lo que se conoce como *yo digital o personalidad virtual* que está fabricada, no a partir de lo que realmente somos y de nuestras singularidades, sino a partir de lo que los algoritmos matemáticos y Big data, consideran que somos.

El problema principal reside en que si bien los datos personales que se utilizan en el análisis predictivo, en principio, aunque no siempre, suelen ser anónimos, se ha llegado a la evidencia de que se pueden llevar a cabo procesos de desanonimización y consecuentemente, llegar a identificar a las personas a quienes tales datos anónimos corresponden. Y los datos personales que circulan por la red y que son sometidos a escrutinio son ingentes. Así los Gobiernos, las empresas o las redes sociales, recopilan datos personales de manera masiva y después realizan una tarea de discriminación o tratamiento de los datos en función de su relevancia o sus intereses. Lo que ha dado lugar a la existencia del llamado *dark data* o mares de datos irrelevantes e inútiles, que son obtenidos y almacenados, pero que, por su escasa entidad y calidad, no sirven para generar resultados óptimos en términos de Big Data. La información circulante crece a un ritmo que se duplica cada año y el 90% de esa información circulante no es analizada ni utilizada de momento. De esta forma sólo el 10% de toda la información generada por los usuarios es susceptible de ser tratada para conformar y utilizar datos de los ciudadanos, pero este porcentaje aumenta en la misma medida en que los dispositivos de Big data se van desarrollando y perfeccionando a través de la Inteligencia artificial.

El derecho a la intimidad aparece recogido en nuestro ordenamiento jurídico en el art. 18. 1 CE: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*. Si bien, en su origen el derecho a la intimidad se configura como un derecho de defensa, *the right to be alone* o derecho a ser dejado en paz en la vida privada frente a las injerencias de terceros; en la actualidad se constituye además como un derecho o potestad que posibilita al individuo decidir sobre lo que quiere que los demás conozcan de lo que le resulta propio. Esta manifestación del derecho a la intimidad como potestad le otorga un carácter fundamentalmente subjetivo. De ahí que el concepto de intimidad resultará diferente para cada ciudadano, grupo, sociedad e incluso momento histórico, siendo "elementos determinantes en su configuración la edad, la cultura, la educación, la comunidad en la que nos integramos. De entre ellos, el elemento de mayor influencia en la determinación del contenido esencial del derecho a la intimidad es la conformación social que de él realiza una sociedad en un momento determinado"[30].

[30] REBOLLO DELGADO, L: *Limites a la libertad de comunicación pública.* Dykinson, 2008, páginas 96 a 113. Sobre la misma materia REBOLLO DELGADO, L: *El derecho fundamental a la intimidad.* Dykinson. 2ª Ed. Madrid 2005.

Reflejo del concepto de intimidad vigente hoy en día en nuestro contexto social es el mostrado a través del comportamiento de las personas en las redes sociales, donde existe una constante y desmedida proyección voluntaria de lo que somos, tenemos y hacemos. Vivimos de manera pública. Reveladora de este nuevo concepto de intimidad que se abre camino con paso firme a través de la entronización de internet en nuestras actividades más cotidianas, es la conclusión de las encuestas sobre las tendencias entre los más jóvenes: los usuarios de 18 a 24 años tienen percepciones sobre la intimidad diferentes al resto, cercanas al concepto de la llamada sociedad de la transparencia, que lleva a la información total, sin permitir lagunas de información, ni de visión.[31]

Se ha acuñado el término *publicy* como término opuesto a *privacy*. Antes elegíamos qué parte de nuestra privacidad queríamos exponer o hacer pública, ahora ocurre al revés, vivimos en público y elegimos qué parte de nuestras vidas mantenemos en privado. O lo que es lo mismo, la configuración por defecto es lo público: *public is the new default*. Esta diferente apreciación de lo que consideramos íntimo o privado es enormemente relevante en términos de Big data, puesto que somos los particulares los que mayor cantidad de datos producimos a través de nuestra actividad en redes sociales, la utilización de whatsapp, el uso de dispositivos móviles o nuestra navegación por la Red y, quienes, en consecuencia, exponemos de manera voluntaria y masiva nuestra intimidad o, lo que, hasta ese momento, considerábamos íntimo.

Un último ejemplo al respecto de lo que venimos analizando, nos lo pone Pariser. Detalla el autor al respecto de los atentados del 11 S, que "inmediatamente después de los ataques, el alcance del complot no estaba muy claro. ¿Había más piratas aéreos que aún no habían sido encontrados? ¿Hasta dónde alcanzaba la red que había perpetrado los ataques? Durante tres días, la CIA, el FBI y un montón de otras agencias con siglas, trabajaron sin descanso para determinar quién más estaba implicado. Se ordenó aterrizar a los aviones de todo el país, se cerraron los aeropuertos. Cuando llegó ayuda, lo hizo desde un lugar improbable. El 14 de septiembre el FBI hizo públicos los nombres de los piratas aéreos y pedía -suplicaba- que cualquiera que tuviera información de los agresores se pusiera en contacto con ellos. Más tarde, ese mismo día, el FBI recibió una llamada de Mack McLarty, un antiguo funcionario de la Casa Blanca, miembro ahora del consejo directivo de una pequeña, aunque lucrativa compañía llamada Acxiom. Tan pronto como se hicieron públicos los nombres de los secuestradores, Acxiom buscó en sus enormes bases de datos, que ocupan dos hectáreas en la diminuta Conway (Arkansas). Encontró información interesante relativa a los culpables de los ataques. De hecho, resultó que Acxiom sabía más sobre once de los dieci-

[31] Es interesante a este respecto la obra de BYUNG-CHUL, H: *La sociedad de la transparencia*. Herder, 2012.

nueve secuestradores que todo el Gobierno de Estados Unidos, incluyendo su pasado, sus direcciones y los nombres de sus compañeros de piso"[32].

Parece claro que el derecho a la intimidad ha evolucionado socialmente, lo que es una característica implícita del mismo, dado el fuerte componente social que le es inherente. Ahora bien, también es palmario que necesita de una reinterpretación jurídica que tape las ausencias de regulación que el tratamiento masivo de datos y la Inteligencia artificial han generado. Aun conscientes del giro a lo público de nuestras vidas generado por internet, no podemos obviar que en el derecho a la intimidad es donde surge la conformación del *yo*, y ámbito donde se gesta la dignidad humana y el libre desarrollo de su personalidad, aspectos todos ellos necesitados de protección jurídica. A ello debemos sumar que este contexto íntimo es donde a su vez se incardinan las raíces de la libertad del sujeto individualmente considerado. Sin este ámbito, el individuo es vulnerable, y como consecuencia de ello, también la sociedad, porque la intimidad sigue siendo el esencial sustrato de la pluralidad social. Eliminar esta protección no únicamente tiene el riesgo de hacernos a todos iguales, sino también de la manipulación o manejo de los individuos por cualquier ideología o interés, y lamentablemente nuestra historia universal es prolija en ejemplos de las consecuencias de la plasmación de esta circunstancia.

Aunque es evidente que el derecho a la intimidad se ha ido acomodando, o quizás mejor expresado, reduciendo en su concepción más reciente, ello no supone problema jurídico si prevalece el elemento esencial de voluntariedad, debido a que como hemos manifestado, el contexto social ahorma de forma muy considerable los límites de la intimidad. Incluso podríamos manifestar que hay una colaboración necesaria del sujeto en ese reduccionismo de la intimidad que internet genera, pero no podemos desposeer por completo al individuo del derecho, o convertirlo en indisponible, o que el uso masivo de datos, combinado con la IA, lo desdibujen por completo. Ello no es solo contrario al ordenamiento jurídico, lo es también a la forma de entender al ser humano y su organización en sociedad. Si desposeemos al individuo de intimidad, lo hacemos también de los elementos esenciales que conforman su personalidad, lo deshumanizamos, creamos seres indiferenciados y manipulables, en definitiva, dejan de ser individuos para constituirse en sujetos de otros.

Es doctrina sentada en el ámbito europeo, tanto por el TEDH y el TJUE, como por nuestro Tribunal Constitucional, en base al principio denominado "calidad de la ley", que toda excepción, o injerencia en la vigencia de los derechos fundamentales, debe estar contemplada en ley formal, de tal manera que ésta debe establecer en qué circunstancias, y en qué condiciones, se pueden producir aquéllos supuestos. Otro principio básico plenamente asentado en los ordenamientos jurídicos occidentales es la interpretación

[32] PARISER, E: *El filtro burbuja,* páginas 50 y 51.

restrictiva de toda limitación de derechos frente al carácter expansivo de la interpretación de su contenido esencial, vigencia y garantías. En la misma línea jurídica está el RGPD, si bien realiza una bifurcación al respecto de esta circunstancia, de forma tal que en unas ocasiones estas excepciones o injerencias justificadas vienen especificadas en el propio RGPD, y en otras se deja a los Estados miembros su determinación o concreción. Estas determinaciones no plantean dificultad de delimitación respecto a intereses públicos, pero es algo más confusa su delimitación en relación con los privados. En algunas ocasiones se delimita de forma concreta, incluso excepcionando el consentimiento, como ocurre en el art 6.1.f)[33]. Como manifiesta Hernández Corchete[34], "… el RGPD no remite al legislador nacional la determinación de cuáles sean estos intereses y de qué condicionantes han de incorporarse en cada ámbito sectorial al tratamiento para que el sacrificio de la privacidad del titular de los datos sea proporcionado … debe entenderse como una proscripción del complemento normativo por el legislador nacional, salvo cuando éste sea expresamente requerido. Esta circunstancia conlleva, en el contexto que ahora nos ocupa, que no sea el legislador quien, luego de ponderar en qué medida procede el sacrificio de la privacidad de los titulares de los datos, disponga los presupuestos y las condiciones de los tratamientos que se admitan como lícitos. Una regulación tan genérica como la del artículo 6.1.a) RGPD deja enteramente para el momento aplicativo la selección de los intereses privados que justifican un tratamiento y la precisión de los términos y condiciones dentro de los cuáles se reputa lícito. Serán las autoridades administrativas de control y luego los tribunales de justicia, con el Tribunal de Luxemburgo como última instancia, quienes realicen caso por caso esta tarea, y la harán con completa libertad porque su decisión no resulta constreñida y ni siquiera guiada por criterios normativamente preestablecidos". De ello no cabe deducir arbitrariedad o inseguridad jurídica, pero sí una ausencia de concreción jurídica, que deberá paliar la jurisprudencia, tanto nacional, como europea, y por tanto, hasta que ello se produzca, es claro el vacío jurídico.

Como puede apreciarse, el derecho fundamental a la intimidad se ha visto constreñido, cuando no manifiestamente vulnerado por la aplicación y

---

[33] Art. 6.1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

[34] HERNÁNDEZ CORCHETE, J. A: *Expectativas de privacidad, tutela de la intimidad y protección de datos*, en la obra de VV. AA: *Sociedad Digital y Derecho*. BOE. Madrid 2018, páginas. 291 y 292.

extensión del uso de Big data y la aplicación de medios de Inteligencia artificial. Ante ello, no hay una respuesta jurídica unitaria, más bien al contrario, muchas vulneraciones de las referidas en este apartado se encuentran en la actualidad en un limbo jurídico, y su garantía depende más de las pretensiones o actuaciones de particulares o empresas privadas, que de la firme pretensión estatal de encajarlas en una normativa protectora o garante del derecho que analizamos. Pero aún en el supuesto de que se diera esa pretensión estatal, sus medios son manifiestamente limitados. Es lugar común hoy para los juristas, reclamar una normativa que tenga carácter global, y que lleve implícita una ejecutividad exenta de toda limitación estatal.

Queda claro que el derecho a la intimidad es el primer y sustantivo damnificado por el uso masivo de datos operado a través de la IA. De igual forma, es palmario que, como barrera de contención, el derecho a la intimidad está literalmente desbordado, tanto sus pilares, como son el consentimiento y la voluntariedad del individuo; como en los aspectos colaterales de su vigencia. Es indudable que la ola del uso de la IA ha desbordado al derecho en su concepción jurídica moderna. El tratamiento actual de los datos hace inoperativa la voluntad del sujeto de mantener fuera del conocimiento público una infinidad de aspectos a él relativos. A ello se añade la problemática de que el mismo sistema operativo trabaja a ciegas con respecto a quién lo elabora, a lo que se suma, que, al tener una finalidad concreta, desconoce los efectos colaterales. De esta forma, en muchas ocasiones no hay una voluntariedad concreta de intromisión en el derecho a la intimidad, pero sí un resultado de vulneración del derecho.

3. Protección de datos de carácter personal

Otro de los derechos fundamentales que puede resultar vulnerado es el derecho a la protección de datos de carácter personal, íntimamente relacionado con el derecho consagrado en el art. 18.1 CE y que el Tribunal Constitucional, por lo que se refiere a nuestro ordenamiento jurídico, configura en la Sentencia 292/2000, de 30 de noviembre de 2000 a partir de la dicción del art. 18.4 CE: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". La sentencia citada configura la llamada libertad informática o derecho a la protección de datos de carácter personal como "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, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos

personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular."

Por lo tanto, si desde el punto de vista de la privacidad, el riesgo que supone el Big data y la Inteligencia artificial sólo afecta a nuestros datos personales reservados, los que hemos elegido no hacer públicos; desde el punto de vista del derecho a la protección de datos, los datos personales afectados son todos, los públicos y privados, lo relevante es que se trata de información que nos identifica o nos pueda identificar. Existe la posibilidad técnica de que, mediante el cruce de datos anónimos, con otras bases de datos, se pueda revelar la identidad de las personas, o de forma genérica revertir la anonimización. Ésta ya no es una técnica irreversible y, por lo tanto, tampoco una garantía absoluta de protección de los datos de carácter personal. Gil González[35] nos pone dos claros ejemplos de sus deficiencias como técnica de protección.

Caso GIC: identificación por el trío código postal, fecha de nacimiento y sexo.

A mediados de los años 90, en Massachusetts, el denominado *Group Insurance Commission* (GIC) decidió hacer públicos datos relativos a las visitas al hospital de los funcionarios públicos, con el objetivo de que los investigadores pudieran analizarlos y sacar conclusiones. El GIC «anonimizó» previamente los datos, mediante la eliminación de identificadores personales explícitos, tales como el nombre, la dirección y el número de la Seguridad Social. Pese a ello, cerca de cien atributos de cada paciente y hospital, permanecieron en los datos hechos públicos; entre éstos, el código postal, la fecha de nacimiento y el sexo de los individuos. En ese momento, el Gobernador de Massachussets, William Weld, aseguró públicamente que la privacidad de los individuos estaba asegurada.

Lantaya Sweeny, directora del Laboratorio de Privacidad de la Universidad de Harvard, realizó un estudio cuyo objetivo era poner de manifiesto las limitaciones de las normas de privacidad y las medidas de seguridad para poder implementar mejoras mediante el uso de algoritmos más fuertes y complejos. Sweeny pidió una copia de los datos publicados y comenzó a intentar reidentificar los datos del Gobernador. Sabía que éste residía en la ciudad de Cambridge (Massachusetts), una ciudad de 54.000 residentes y siete códigos postales. Además, pagando 20 dólares compró el último censo electoral de la ciudad de Cambridge, que contenía, entre otros datos, el nombre, dirección, código postal, fecha de nacimiento y sexo de cada votante. Combinando ambas bases de datos, los datos de GIC y el censo electoral, Sweeny consiguió identificar al Gobernador Weld sin dificultad: únicamente seis personas en Cambridge habían nacido el mismo día que el Gobernador,

[35] GIL GONZÁLEZ, E: *Big Data, privacidad y protección de datos.* AEPD. Madrid 2016, páginas 104 y siguientes.

solo tres de estas personas eran hombres, y solamente él vivía en su código postal. Sweeny envió el historial médico del Gobernador, que incluía diagnósticos y prescripciones, a su oficina. Pero Sweeny, no se quedó ahí. Extendió sus análisis hasta concluir que el 87.1% de los ciudadanos residentes en Estados Unidos son identificables mediante este trío de atributos: código postal, fecha de nacimiento y sexo.

Las conclusiones del experimento de Sweeny sobre este trío de identificadores han vuelto a ser analizadas y actualizadas. En un estudio llevado a cabo en la Universidad de Standford, se comprobó que en 2006 la proporción de personas residentes en Estados Unidos que podían ser reidentificadas utilizando únicamente la triada código postal, fecha de nacimiento y sexo había descendido al 63.3%. No obstante, el nuevo estudio volvió a demostrar que los ataques de reidentificación siguen siendo fáciles de realizar. Además, es necesario tener en cuenta que la disponibilidad de información que actualmente es pública es mucho mayor que en el momento en que se realizó el estudio, y las técnicas de reidentificación son más exactas, de modo que es fácil imaginar que quien tenga pretensión de hacerlo, pueda tener acceso a más datos que el código postal, la fecha de nacimiento y el sexo de las personas cuyos datos se encuentran en la base de datos.

Caso Netflix: El segundo caso que expone la autora que venimos citando, es el denominado caso Premio Netflix. Ésta, es la mayor empresa del mundo proveedora, a través de una tarifa plana mensual, de contenidos multimedia (películas y series de televisión). En octubre de 2006, la compañía lanzó el denominado Premio Netflix. La empresa hizo públicos cien millones de registros de películas de 500.000 usuarios, y ofreció una recompensa a aquel que consiguiera mejorar su servicio de recomendación de películas (que se basa en las películas que otros usuarios con gustos similares puntuaron de forma muy alta). Los datos habían sido anonimizados, de forma que se eliminaron todos los identificadores personales, excepto las calificaciones de las películas y la fecha de la calificación; además, se añadió ruido (distorsionadores), de forma que las calificaciones de los usuarios fueron ligeramente incrementadas o reducidas. Como fuente de datos externa se utilizó la base de datos pública denominada *Internet Movie Database* (IMB), una base de datos online que almacena información relacionada con películas. La cuestión de la que partía el experimento era: ¿cuánto tiene que saber un adversario sobre un suscriptor de Netflix para poder identificar sus datos en la base de datos, y así, conocer su historial completo de películas? Es decir, en términos analíticos el estudio se basó en calcular el tamaño de los datos auxiliares que eran necesarios para reidentificar a los sujetos supuestamente anonimizados.

En este sentido, cabría preguntarse si realmente un suscriptor de Netflix considera privado su historial de películas vistas. Incluso aunque la respuesta fuera negativa (lo cual no se puede asumir), eso sería así solo en la medida en que no comprendamos las consecuencias reales de reidentificar estos

datos. Tal y como demostró el experimento, la correlación encontrada entre la base de datos anonimizada del Premio Netflix y la base de datos pública de IMB permite conocer información sensible y no pública sobre una persona, tal como preferencias políticas u orientación sexual. En efecto, se logró identificar a uno de los usuarios, una madre de familia lesbiana que mantenía su orientación sexual en secreto, residente en una región muy conservadora de Estados Unidos, y que demandó a la empresa bajo el pseudónimo de Jane Doe. Tras el escándalo, investigadores de la universidad de Texas compararon los datos de Netflix con otros datos públicos sobre calificación de películas. El estudio demostró que un usuario que hubiera calificado tan solo seis películas poco conocidas (de una lista de quinientas películas), podría ser identificado en el 84% de los casos. Y esta proporción aumentaba al 99% de los casos si, además, se sabía en qué fecha se habían calificado las películas. Así, se demostró que la calificación de las películas creaba una huella personal. Antes de este momento, nadie habría intuido que participar en una encuesta anónima al respecto de películas, pudiese revelar datos de identificación personal. En ambos casos fue necesario combinar dos bases de datos que contenían datos parciales sobre las personas, y que muestra el principio de que, a pesar de que una base de datos parezca anónima, cuando se compara con una segunda base de datos, se encuentra información única sobre los sujetos, y la reidentificación de éstos se hace posible.

De la problemática en relación con el uso del Big data se han hecho eco muchos organismos e instituciones, como ejemplo traemos el de la Agencia Española de Protección de Datos que, en su Memoria de 2013, manifestaba lo siguiente: "… estos tratamientos encierran notables riesgos para los derechos de los individuos. Los Big data –se utilizan las dos pronunciaciones, en inglés y español– se emplean principalmente para hacer predicciones basándose en correlaciones, y tratan el qué, tratan de qué está ocurriendo o de qué va a ocurrir, pero no el porqué, por qué se han producido o por qué se van a producir. Con ello se pueden extraer conclusiones sobre individuos, señalar su proclividad a determinadas conductas, predecir su probabilidad de encontrarse en determinados estados –situaciones económicas, enfermedades, etcétera–; predicciones y conclusiones que, como fácilmente puede advertirse, tienen un enorme impacto sobre el libre desarrollo de las personas, tanto si son incorrectas como si son correctas, y aquí está uno de los aspectos más preocupantes. Entrañan un alto riesgo de discriminación y, en todo caso, son merecedoras de todos los reproches y las prevenciones que cabe hacer a cualquier clasificación de individuos por categorías".

En definitiva, y como nos recuerda Hoffmann-Riem, la aplicación e interpretación del Derecho no nos asegura "en modo alguno que tales posibilidades del ordenamiento jurídico de reaccionar con flexibilidad a los nuevos desarrollos puedan hacer frente plenamente a las bruscas transformaciones fundamentales como las que origina en la actualidad la transformación digi-

tal de la sociedad. Si no es este el caso, hay necesidad de modificar el ordenamiento jurídico" [36].

La protección de datos de carácter personal, y su amplia regulación, tanto en algunos Estados, como en la Unión Europea, tampoco se establece como una limitación adecuada en los supuestos de Big data y su tratamiento a través de Inteligencia artificial. En primer lugar, la propia normativa abre grandes portillos jurídicos a la exclusión, como hace el art. 6.4 RGPD, a las que hay que añadir las excepciones del art. 9.2 de la misma norma.

Otro gran portillo jurídico proviene de la clave de bóveda en que se constituye el consentimiento en la normativa actual. A pesar de la rotundidad del apartado 11 del art. 4 del RGPD, de la claridad del art. 7, y las interpretaciones que formulan los Considerandos 42 y 43, la realidad es bien distinta. Al prestar el consentimiento, en la mayoría de las ocasiones el usuario no tiene otra alternativa de mercado. A ello hay que añadir que la inmensa mayoría de los procesos de prestación del consentimiento van insertos en un conjunto de condiciones unilaterales, es decir, un contrato de adhesión, en virtud de lo cual no le cabe al usuario la posibilidad de negociación entre partes iguales, sino que únicamente puede optar entre el todo o la nada.

Un elemento añadido distorsionador de la vigencia de la protección de datos en el ámbito de la Big data e Inteligencia artificial, proviene de la propia indefinición de la norma, que recurre en muchas ocasiones a conceptos jurídicos indeterminados, en cuya interpretación caben amplias líneas de aplicación, y que requerirán de precisiones jurídicas, ya sean de las resoluciones judiciales, o de las autoridades de control. Pero mientras ello se produce, la puerta está abierta, la vulneración es posible y la lesión del derecho está prácticamente garantizada.

Otro problema respecto del consentimiento es la amplitud interpretativa que aplica aquél que lo recaba. De esta forma se indetermina la finalidad del tratamiento, lo que deja en manos del responsable su interpretación, aplicación o uso. Incluso esta interpretación extensiva puede hacer que un usuario otorgue consentimiento respecto de datos que no son de su titularidad, y por lo tanto, sobre los que no tiene derecho de disposición. Esto ocurre con la entrega de datos, o metadatos, de terceros en una comunicación o en una red social, donde el tercero es un mero interlocutor. La misma circunstancia se produce con la combinación de datos a través de tratamientos masivos, donde se agregan grupos de datos y se obtienen resultados de tendencias, nivel económico, predisposiciones u otra infinidad de perfiles, que a su vez pueden ser revendidos y sobre los que se añaden otras bases de datos masivas y sobre los que se aplican otros algoritmos. Recuérdese que una de las características del Big data es que el uso de los datos no se agota con un tratamiento, sino que los datos pueden estar sometidos a infinitos procesos

[36] Obra citada, pág. 79.

para la obtención de los resultados pretendidos, incluido el de la reidentificación. El uso de los datos y metadatos de terceros es muy frecuente en las redes sociales. Así ocurrió en EE. UU. en 2018 con Facebook, donde bajo la calificación de robo, los datos de 87 millones de usuarios fueros usados por una empresa (Cambridge Analytica) para apoyar la campaña electoral del presidente de EE. UU. D. Trump. La mayoría de los datos no eran de los concretos usuarios de Facebook, sino de personas con quienes éstos se habían comunicado a través de la función "me gusta".

La entrada en vigor del Reglamento UE 868[37] apunta de forma muy clara la inclusión de los datos en el ámbito del mercado único en la UE, así como su valor intrínseco, al que se añade la reutilización infinita. Pese a que su objeto se circunscribe a las Administraciones públicas, se establece la figura de los servicios de intermediación de datos, entre los titulares de los mismos y los potenciales usuarios, y que como establece el art. 10 "estos servicios podrán comprender el intercambio bilateral o multilateral de datos o la creación de plataformas o bases de datos que posibiliten el intercambio o la utilización en común de datos, así como el establecimiento de otra infraestructura específica para la interconexión de los titulares de datos con los usuarios de datos".

La comercialización de datos es ya una realidad normativa y mercantil. La UE consciente del valor de este mercado ha establecido ya las bases de su regulación, pero se hace desde una perspectiva de mercado, de regulación mercantil, sin primar la defensa de los derechos y libertades fundamentales, sin que suponga tal afirmación que los desdeñe o soslaye en su vigencia, pero sí se observa con claridad que no es el objeto troncal de la regulación.

Un último aspecto para considerar es que tanto el RGPD, como las regulaciones de los Estados miembros, desconocen la posibilidad de articular mecanismos de remuneración al usuario cuando presta el consentimiento de datos que tienen un especial valor económico, partiendo siempre de la idea de que todos los datos tienen valor. Parece adecuado que dado lo lucrativo del mercado de datos, este pudiera revertir parte de su productividad en sus titulares. A esta posibilidad viene oponiéndose de forma sistemática la Unión Europea, argumentado que sería mercantilizar un derecho fundamental, pero no debemos olvidar que otros derechos fundamentales son objeto de comercio, como ocurre con el derecho a la imagen. El atribuir la propiedad de los datos a su titular haría variar la protección al ámbito civil, que, en todo caso, se manifiesta como más garantista que la plena indefensión ante el uso y comercio de los datos existentes en la actualidad. Una interesante teoría al respecto de patrimonializar los datos, es la ofrecida por Ottolia, para quien la protección de la propiedad intelectual, dado su carác-

[37] Reglamento UE 2022/868 del PE y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento UE 2018/1724 (Reglamento de Gobernanza de Datos).

ter universal y sus desarrollados mecanismos de efectividad, puede suponer una alternativa como vehículo para patrimonializar los datos[38].

Es conveniente referenciar, por último, la protección desde el diseño y por defecto. Como nos indica Gil González, "Los sistemas de privacidad desde el diseño implican que las tecnologías son construidas teniendo en cuenta la necesidad de la protección de la privacidad. Por su parte, los sistemas de privacidad por defecto conllevan que la tecnología está configurada para que las opciones que por defecto vienen establecidas sean las más protectoras de la privacidad; y el individuo puede posteriormente cambiar la configuración para permitir otras utilidades que requieran un nivel de privacidad menor.

La mejor aproximación será incluir la configuración más segura por defecto en un sistema diseñado bajo los principios de privacidad desde el diseño. De este modo, los avances persiguen mantener todo el potencial de crear valor de las tecnologías, poniendo la protección del individuo como un factor más a tener en cuenta, junto con el resto de los parámetros (como capacidad operativa, viabilidad económica, etc.). Así se crea una dinámica *win-win* (es decir, en la que ganan ambas partes) para las organizaciones y los individuos"[39].

Recordemos que el RGPD, en su artículo 25, establece que: "1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

El Considerando 78 del RGPD establece que "… Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos persona-

[38] OTTOLIA, A: *Derecho, Big data e Inteligencia artificial.* Tirant lo Blanch. Valencia 2018, páginas 85 y siguientes.

[39] GIL GONZÁLEZ, E: *Big Data y protección de datos.* AEPD y BOE. Madrid 2016, pág. 125.

les, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos".

Como puede verificarse, son muchas las incógnitas y pocas las soluciones. Es evidente que la normativa actual de protección de datos adolece de una regulación integral que solvente la problemática introducida por la aplicación de Inteligencia artificial a bases de datos masivas. En la actualidad puede afirmarse que la regulación alcanza, y con dificultad, a la protección de datos de carácter personal para un uso normalizado de los mismos, pero es manifiestamente insuficiente más allá de la prescripción de si el dato está referido a una persona identificada o identificable. Si a ello añadimos la reversibilidad de las técnicas de anonimización, la conclusión es aún más rotunda, hay cierta protección sobre los datos de carácter personal, pero ninguna sobre el resto de datos, pero lo alarmante es que éstos rompen la protección jurídica de los primeros a través del tratamiento masivo con IA, lo que se constituye en una inquietante realidad, el mecanismo más técnico, mejor perfilado para la garantía de los derechos fundamentales en relación con las nuevas tecnologías, se ve manifiestamente vulnerado por las nuevas técnicas de IA.

4. Libertad ideológica

La influencia que tiene la existencia de Big data y la Inteligencia artificial es también muy significativa en la libertad ideológica, tanto de forma directa al propio derecho, como en otros muchos aspectos de la organización social, sobre los que destaca la esencia de la democracia, o de forma algo más genérica, la organización política.

Aunque la libertad ideológica está íntimamente correlacionada con la libertad de expresión e información, hemos querido dedicar apartados de análisis diferentes, puesto que la libertad ideológica tiene a nuestro juicio una esencial importancia en la conformación de nuestra sociedad actual, a la vez que se producen efectos diferenciados con respecto a la libertad de expresión e información.

Es lugar común en la doctrina, esencialmente en la sociología y en la ciencia política, alinearse con las dos posturas mayoritarias en el análisis de

la influencia de las nuevas tecnologías respecto a libertad ideológica. Por un lado, se postula que Internet es un ámbito de libertad, y libre actuación que escapa al control de los Estados y de los poderosos intereses existentes a nivel global, por lo cual el individuo accede a una infinita cantidad de información para elaborar sus propias convicciones y conformar su ideología en plena libertad; por otro, se manifiesta lo ilusoria de esta concepción puesto que la Red no es neutra, y está sometida a los mismos intereses que existen fuera de ella, e incluso se controla de forma más sencilla que la vida real, independientemente de que los impulsos sean políticos, ideológicos o comerciales. Muchos de estos planteamientos se centran no tanto en la propia libertad ideológica, y sí más bien en el concepto y evolución que tendrá la democracia con el uso de Internet.

A nuestro juicio la libertad ideológica es su configuración actual en los países democráticos es uno de los pilares sobre el que se asienta la ordenación social. La dignidad de la persona y el libre desarrollo de la personalidad tienen su concreción en la libertad ideológica, a la vez que ésta es elemento esencial de conformación del pluralismo en el sentido más amplio del término. A ello se añade en la mayoría de los ordenamientos jurídicos occidentales, la limitación de la imposibilidad de discriminación por razón de opinión, y la exención de declarar sobre la propia ideología. Tiene así la libertad ideológica un carácter absoluto, si bien se limita su aplicación o materialización. A juicio de nuestro Tribunal Constitucional, la libertad ideológica como derecho subjetivo tiene una perspectiva interna y otra externa. La primera viene constituida por el derecho de todo individuo a "adoptar una determinada posición intelectual ante la vida y cuanto le concierne y a representar o enjuiciar la realidad según sus personales convicciones". Desde la perspectiva externa el Tribunal Constitucional configura este derecho como la opción del individuo a una actuación conforme a sus ideas y convicciones sin por ello "sufrir sanción o demérito, ni padecer la compulsión o injerencia de los poderes públicos"[40]. Desde la perspectiva ideológica, al Estado le corresponde mantener una posición de neutralidad, no le está permitido valorar, posicionarse o mantener una ideología concreta, puesto que la libertad ideológica, como hemos manifestado, adquiere una dimensión institucional, al ser el fundamento del pluralismo político que establece el art. 1.1 CE como uno de los valores superiores de nuestro ordenamiento jurídico.

Pero es también relevante en este derecho, y dentro del contexto que nos ocupa, la relación entre particulares. A este respecto opera la limitación del inciso final del art. 16.1 CE "necesaria para el mantenimiento del orden público protegido por la ley". Este concepto jurídico indeterminado se muestra hoy poco eficaz, máxime teniendo en cuenta que la sociedad digital ha variado de forma muy significativa el origen de las vulneraciones o limitaciones del derecho que nos ocupa. De esta forma, los poderes públicos son

[40] STC 120/1990, f. ju. 10.

en esencia árbitros del ejercicio de la libertad ideológica, dado que las vulneraciones provienen esencialmente de la actuación de particulares. El Estado es hoy en esencia más un garante de su vigencia, que sujeto activo de sus vulneraciones. Indudablemente esta afirmación cabe matizarla o concretarla al respecto de aquellos Estados que entran dentro de unos cánones democráticos, y siempre siendo conscientes que existen excepciones ocasionales a esta afirmación. En todo caso, no constituyen el grueso de los quebrantos normativos, pero afirmando a la vez, que no supone ello su inexistencia.

De esta forma, hemos de concluir que hoy la vulnerabilidad de la libertad ideológica proviene esencialmente de particulares, a la vez que, de otros Estados no democráticos, y los riesgos son muy variados. Sin pretender hacer relación exhaustiva de los mismos, sí referenciaremos aquellos que entran en directa correlación con el uso de Big data y la Inteligencia artificial.

La consecuencia más evidente a este respecto es que los generadores e intermediarios de la información necesitan muy pocos recursos para realizar análisis automatizados, o tratamientos de esta que puedan obedecer a una multiplicidad de pretensiones, entre las que destaca la personalización de la información. Opera aquí de forma contundente el concepto de filtro burbuja que utiliza Pariser, de tal forma que internet nos va ofreciendo un conjunto informativo, o de canales de información, en función de nuestros gustos o de nuestras interacciones en la Red. Ello supone limitar de forma sustantiva nuestro mundo de acceso informativo, a la vez que hay que deducir que el rastro en la navegación que vamos dejando es objeto de tratamiento o manipulación, lo que a su vez condiciona el ofrecimiento de información que se nos realiza. Aunque si bien es cierto que esto es subsanable por el sujeto, también lo es que requiere una actividad complementaria y un plus de objetividad por parte del individuo.

Otro mecanismo de tratamiento de la información se concreta en la creación de tendencias, que tienen una directa repercusión en la opinión pública, y como consecuencia de ello, incluso pueden generar de forma artificial opiniones que sean mayoritarias (a lo que se denomina realidad aumentada). También existe la posibilidad de generación de noticias falsas que, aún, no teniendo una tendencia cuantitativa en la formación de la opinión pública, suelen generar desinformación o una clara confusión de ésta. En resumen, y como afirma Hoffmann-Riem "en la medida en que el manejo de datos permite el desarrollo del poder político o social de un modo que resulta problemático bajo aspectos del Estado socialdemocrático de Derecho, es importante que se establezcan mecanismos eficaces para contrarrestarlo jurídicamente"[41].

Si bien la actividad del Estado está sometida a un alto grado de control de transparencia, no ocurre lo mismo con la actividad empresarial, singular-

[41] Obra citada, pág. 121.

mente en lo que se refiere a la obtención y explotación de la información. De esta forma es frecuente que se imposibilite o se niegue el acceso a los procesos de tratamiento de la información, a la vez que tampoco se permite el control externo efectivo que constate una realización de buenas prácticas, o de no vulneración del ordenamiento jurídico, incluso en los supuestos en que se ven afectados intereses o derechos individuales y colectivos. Este control, necesariamente debería producirse sobre los algoritmos utilizados para el tratamiento y obtención de la información, y debe concretarse en las finalidades de aquéllos, al objeto de verificar que son acordes con el ordenamiento jurídico.

Las empresas son muy celosas de estas actividades y a su vez en la mayoría de los países occidentales, paradójicamente están protegidas por el propio ordenamiento jurídico. Pensemos por ejemplo en las fórmulas que utiliza una empresa farmacéutica para la elaboración de un medicamento, o en la que usa una compañía de refrescos. Aquí el Estado realiza un control de la elaboración, producción y también de sus productos, con objeto de verificar que, en todo caso, no sean perjudiciales para el ciudadano, y de serlo, prohibirá su producción y comercialización. Pero esta circunstancia no es trasladable al ámbito de la información, lo que puede suponer una lesión de la libertad ideológica, y como consecuencia directa de ello, un falseamiento del pluralismo ideológico y político, que a su vez tiene una muy negativa repercusión en la organización social. Debemos recordar aquí que la libertad ideológica se constituye en el pilar del desarrollo de las sociedades democráticas, y a la vez en el engranaje imprescindible del libre desarrollo de la personalidad. Si limitamos o anulamos estos derechos, retrotraemos al individuo a la categoría de súbdito, y usamos para ello la tecnología. Como manifiesta Pariser, "cuanto más poder ostentamos sobre nuestro propio entorno, más poder tienen sobre nosotros quien asume el control"[42].

En nuestro ordenamiento jurídico, el Tribunal Constitucional ha tenido ocasión de poner de manifiesto aspectos esenciales de una adecuación de la libertad ideológica a las necesidades actuales. De forma concreta la STC 76/2019[43], delimita los nuevos contornos de este Derecho, y merece una aproximación a sus contenidos. Para el Tribunal, y después de recordar que a la libertad ideológica se la califica de categoría especial de dato en el art. 9 del RGPD, entiende que la protección de datos realiza en ocasiones una función instrumental de otros derechos fundamentales, y de forma concreta en el caso que se analiza en esta sentencia, respecto a la libertad ideológica.

---

[42] Obra citada, pág. 216.

[43] STC 76/2019, de 22 de mayo de 2019, f. ju. 5. Que resuelve el recurso de inconstitucionalidad planteado por el Defensor del Pueblo en relación con el art. 58 bis de la Ley Orgánicas de Régimen Electoral General, en su redacción dada por la LO 3/2018 de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales. El objeto del recurso es la posibilidad de los partidos políticos de tratar datos de los electores "en el marco de sus actividades electorales" y que es declarado inconstitucional.

Manifiesta así, que "… c) La libertad ideológica consagrada en el artículo 16 CE tiene una dimensión positiva, pues se protege «sin más limitación, en sus manifestaciones, que la necesaria para el mantenimiento del orden público protegido por la ley» (apartado 1), y también una dimensión negativa, pues incluye el derecho de toda persona a no «ser obligado a declarar sobre su ideología» (apartado 2).

En síntesis, la libertad ideológica comprende «la proclamación de ideas o posiciones políticas propias o adhesión a las ajenas» (STC 235/2007, de 7 de noviembre, FJ 9), tanto individual como colectivamente, así como la posibilidad de abandonarlas o cambiarlas por otras en todo momento, pero también el secreto o silencio sobre las ideas o posiciones políticas propias, sin ser objeto de coacción o perturbación alguna antes o después de su proclamación o modificación, ni derivada del silencio libremente elegido.

Este Tribunal ha tenido ocasión de destacar la importancia del derecho consagrado en el artículo 16.1 CE. Como afirmamos en la STC 20/1990, de 20 de febrero, FJ 3: «sin la libertad ideológica consagrada en el artículo 16.1 CE, no serían posibles los valores superiores de nuestro ordenamiento jurídico que se propugnan en el artículo 1.1 de la misma para constituir el Estado social y democrático de derecho que en dicho precepto se instaura».

Asimismo, en la STC 120/1992, de 27 de junio, FJ 8, aludimos a la faceta externa de ese derecho en los siguientes términos: «la libertad ideológica […] no se agota en una dimensión interna del derecho a adoptar una determinada posición intelectual ante la vida y cuanto le concierne y a representar o enjuiciar la realidad según personales convicciones. Comprende, además, una dimensión externa de *agere licere*, con arreglo a las propias ideas sin sufrir por ello sanción o demérito ni padecer la compulsión o la injerencia de los poderes públicos».

Después de recordar el Tribunal que la necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, y hacer repaso de la normativa al respecto, el fundamento jurídico 6 se centra en el establecimiento de las garantías para que "el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías que resulten constitucionalmente exigibles en cada caso dependerán de tres factores esencialmente: el tipo de tratamiento de datos que se pretende llevar a cabo; la naturaleza de los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo de tratamiento y a la categoría de datos de que se trate. Así, no plantean los mismos problemas una recogida de datos con fines estadísticos que una recogida de datos con un fin concreto. Tampoco supone el mismo grado de injerencia la recopilación y el procesamiento de datos anónimos

que la recopilación y el procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la salud, la vida sexual, o la orientación sexual de una persona física, que el tratamiento de otro tipo de datos".

Continúa manifestando el Tribunal, que "… el nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales". De esta forma concluye el TC que "… las opiniones políticas son datos personales sensibles cuya necesidad de protección es, en esa medida, superior a la de otros datos personales. Una protección adecuada y específica frente a su tratamiento constituye, en suma, una exigencia constitucional, sin perjuicio de que, como se ha visto, también represente una exigencia derivada del Derecho de la Unión Europea. Por tanto, el legislador está constitucionalmente obligado a adecuar la protección que dispensa a dichos datos personales, en su caso, imponiendo mayores exigencias a fin de que puedan ser objeto de tratamiento y previendo garantías específicas en su tratamiento, además de las que puedan ser comunes o generales".

Continuando con el análisis de la STC 76/2019, es relevante la argumentación al respecto de la inconstitucionalidad de la nueva redacción dada al art. 58 bis de la LOREG por la Ley Orgánica 3/2018. Se manifiesta que "a) La primera tacha de inconstitucionalidad que se dirige a la disposición legal impugnada es que no especifica el interés público esencial que fundamenta la restricción del derecho fundamental. b) La segunda tacha de inconstitucionalidad que se dirige a la disposición legal impugnada es que no limita el tratamiento regulando pormenorizadamente las restricciones al derecho fundamental. La disposición legal impugnada solo recoge una condición limitativa del tratamiento de datos que autoriza: la recopilación de datos personales relativos a las opiniones políticas de las personas solo podrá llevarse a cabo «en el marco de sus actividades electorales». Se trata de una condición que apenas contribuye a constreñir el uso de la habilitación conferida. De una parte, el desarrollo de las actividades electorales no tiene por qué contraerse al proceso electoral, expresión que, en cambio, es la utilizada en el apartado 2 del artículo 58 bis LOREG. De otra, los procesos electorales son relativamente frecuentes en nuestro sistema político. Más allá de la citada condición («en el marco de sus actividades electorales»), la disposición legal impugnada carece de reglas sobre el alcance y contenido de los tratamientos de datos que autoriza". Continúa manifestado el Tribunal, en su fundamento jurídico 9, que "De lo anterior se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia,

ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales.

De esta forma, se han producido tres vulneraciones del artículo 18.4 CE en conexión con el artículo 53.1 CE, autónomas e independientes entre sí, todas ellas vinculadas a la insuficiencia de la ley y que solo el legislador puede remediar, y redundando las tres en la infracción del mandato de preservación del contenido esencial del derecho fundamental que impone el artículo 53.1 CE, en la medida en que, por una parte, la insuficiente adecuación de la norma legal impugnada a los requerimientos de certeza crea, para todos aquellos a los que la recopilación de datos personales pudiera aplicarse, un peligro, en el que reside precisamente dicha vulneración y, por otra parte, la indeterminación de la finalidad del tratamiento y la inexistencia de «garantías adecuadas» o las «mínimas exigibles a la Ley» constituyen en sí mismas injerencias en el derecho fundamental de gravedad similar a la que causaría una intromisión directa en su contenido nuclear".

En definitiva, este análisis jurisprudencial nos pone de manifiesto como el tratamiento de datos puede constituir un elemento necesario para la vulneración del derecho a la libertad ideológica. El individuo queda sometido, como sujeto pasivo, a un tratamiento-manipulación de la información que elude la objetividad, y como consecuencia vicia el ejercicio del derecho a la libertad ideológica. Es tanto como contaminar la fuente que abastece al individuo en la conformación más absoluta del mismo, la ideológica. Ello contamina a su vez el pluralismo en todos sus ámbitos, político, social, ideológico, religioso y moral. Para eludir aquella manipulación, el sujeto debe realizar un esfuerzo significativo de formación, de cultura, que acceda a fuentes diversas de conocimiento, compare y realice una identificación o separación de lo objetivo y de lo subjetivo. Quizás sea ello una actividad desproporcionada en un mundo tecnológico, que demanda inmediatez, donde lo instantáneo es lo adecuado, y donde la saturación de información produce desinformación. Aquí triunfan los eslóganes, los titulares de periódicos, la información sin elaboración. Todo ello tiene una nefasta repercusión individual, y como consecuencia de ella, social.

Es evidente que la tecnología de Big data que alimenta a la Inteligencia artificial ha producido ya un gran deterioro de la conformación ideológica de los ciudadanos, al igual que se aprecian ya iguales síntomas en la organización social, lo que es tanto como reconocer que tenemos ya afectadas las cuadernas de la nave, y las soluciones no se tornan sencillas.

Aunque lo hemos apuntado de forma tangencial, merece en este apartado hacer una pequeña reflexión al respecto de la libertad ideológica, del concepto de globalización. La ordenación social de carácter mundial se sub-

divide hoy claramente en dos mundos, el occidental, donde prima en mayor o menor grado la democracia y la vigencia de los derechos; y el autocrático, que se sumerge en un oscurantismo informativa tergiversado. La globalización ha interconectado estos dos mundos, y ello tiene aspectos positivos y negativos. En los primeros cabe reseñar el conocimiento extenso que puede conseguirse de países que hasta hace poco no teníamos ni referencia de su existencia, a la vez que ellos pueden tener conocimiento de la existencia de otras formas de ordenar la vida social. El elemento más negativo para occidente es la vulnerabilidad respecto de la información o desinformación. Cada vez son más conocidas las claras evidencias de interacción de los regímenes autocráticos en los democráticos a través de los medios de información y comunicación. De forma más concreta cabría hablar de desinformación, o de generar confusión informativa. Las *fake news* son hoy en día un problema relevante, tanto a nivel estatal, como individual, y tienen como objetivo minar la libertad ideológica del ciudadano. Se constituye en un riesgo cierto para el Estado, para la organización social, y también para el individuo, ataca el corazón del Estado social y democrático de Derecho, y a lo más radical en la libre configuración de la persona. La facilidad con la que opera aquí la IA es asombrosa.

A esta palpable práctica de desinformación de los regímenes autocráticos se suman otras muchas, como son los intereses comerciales, la presión ideológica que realizan los *lobbys* o grupos de interés, y los intereses geopolíticos, entre otros. En definitiva, la ideología es objeto de un conglomerado de intereses alejados de la objetividad o la neutralidad, y donde no sólo al individuo le es difícil entresacar conclusiones claras, sino que afecta también al Estado, que es igualmente sujeto pasivo de esta tensión.

La circunstancia expuesta no es novedosa, es propia de la condición humana y acompañado al hombre desde el origen de su existencia, pero la novedad y por consiguiente, el peligro, es ahora la facilidad para desdibujar los elementos que históricamente hemos utilizado para conformar la ideología. Las herramientas clásicas, la mentira, la distorsión de la realidad, la retorsión del lenguaje, la posverdad, entre otras, se ven catapultadas por el uso de la IA, y se hace ello con una manejabilidad y con una eficacia asombrosa. El algoritmo es un fiel servidor de su creador, es una potentísima herramienta de control y de materialización del poder en la más amplia concepción del concepto.

Aunque sería más propio de un análisis sociológico de como se conforma hoy la ideología, parece evidente que el camino clásico que era la formación intelectual, o determinados contextos de formación (la tribu, la familia, el grupo, la sociedad) estos están variando en la actualidad, de igual forma que han variado los medios de acceso a la información y el conocimiento, o en todo caso, aunque persisten estas estructuras, su contenido nuclear se ve modificado por el uso de las nuevas tecnologías, y ello tiene una directa influencia en la manera en que se accede a contenidos que conforman la ideología, pero también en lo que respecta a como se reconfigura, a como se adapta o

acomoda. Parece evidente que el individuo tiene hoy una mayor dificultad para estructurar su ideología, para componer su visión en lo personal y en lo global.

5. Derecho a la información y libertad de expresión

La libertad de información y expresión constituye otro elemento troncal en nuestro sistema social, que puede verse afectado por el uso de Big data y la Inteligencia artificial, y que lo ha sido ya por la irrupción de Internet. El mundo de la información ha venido estando copado por grupos de información muy potentes, tanto en prensa, radio y televisión, y con una fuerte dependencia empresarial e ideológica, que configuraba la opinión pública. El ciudadano ha sido usuario indolente de su producción, y a la vez receloso de esta dinámica, y los ordenamientos jurídicos han entendido siempre la diversidad como garantía de pluralismo democrático, a la vez que exigía ciertas garantías en el ejercicio de la información, por ser una actividad profesionalizada. Por ello nuestro Tribunal Constitucional ya afirmaba en 1987 que la protección constitucional de las libertades comunicativas "alcanza su máximo nivel cuando la libertad es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de la opinión pública que es la prensa entendida en su más amplia acepción"[44]. Internet ha variado de forma radical esta realidad, y ahora la opinión pública se conforma parcialmente al modo clásico, es decir, proveniente de los grandes grupos de comunicación, pero a la vez el usuario de internet es también productor, emisor y receptor de información. Esta información está desprovista de la profesionalidad de los medios clásicos, a la vez que se desconocen en la mayoría de las ocasiones las pretensiones ideológicas o los intereses que las promueven. Ese gran entorno de libertad que constituye Internet, tiene una cara buena de fundamento de libertad, y otra indefectiblemente peligrosa, de manipulación y control informativo, que en la mayoría de las ocasiones se materializa en desinformación. Como manifiesta Capodiferro "recurrir al carácter de garantía institucional del sistema democrático que se ha atribuido a las libertades comunicativas para justificar una interpretación restrictiva de sus límites cuando se ejercen por particulares con un alcance que trasciende el entorno más cercano del sujeto activo o, directamente, defender la ausencia de controles sobre su ejercicio a través de Internet es realizar un brindis a una falsa libertad. Tal cosa supone privilegiar sin una justificación razonable la posición subjetiva del comunicante sobre la de quien ve vulnerado sus derechos a consecuencia de su actuación, ya sea como receptor del mensaje o como titular de un derecho de la esfera personal que resulta lesionado por el contenido de la comunicación"[45].

---

[44] STC 165/1987, f. j. 10.

[45] CAPODIFERRO CUBERO, D: "La libertad de información frente a Internet". Revista de Derecho Político de la UNED nº 100, de 2017, pág. 710.

Como puede comprobarse, nuevas circunstancias, generan nuevos problemas. Por ello es conveniente hacer repaso de los contenidos doctrinales y jurisprudenciales troncales en esta materia.

Como nos recuerda Salvador Martínez[46], "… Tradicionalmente, las Declaraciones de Derechos recogidas en textos constitucionales o en Tratados internacionales garantizaban un único derecho a la libertad de expresión, pero entendida ésta en un sentido amplio, como libertad comprensiva de las diferentes «libertades» que podía ejercer un ciudadano en tanto que emisor en cualquier proceso de comunicación: la libertad de expresar opiniones, la libertad de transmitir noticias, la libertad de expresarse artísticamente, la libertad de transmisión de conocimientos, etc... Posteriormente, algunas Constituciones y Declaraciones de Derechos reconocieron la existencia autónoma de la libertad de información respecto de la libertad de expresión. Y las Constituciones más modernas, entre las que se encuentra la nuestra, no sólo reconocen expresamente la libertad de información, como derecho fundamental autónomo, aunque estrechamente vinculado a la libertad de expresión, sino también la existencia de un derecho a la información. En efecto, la Constitución Española reconoce, por un lado, en el artículo 20.1.a) el «derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción» y, por otro lado, en el arto 20.1.d), el «derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión».

Nuestro Tribunal Constitucional ha manifestado con rotundidad, que el derecho a recibir información "es en rigor una redundancia (no hay comunicación cuando el mensaje no tiene receptor posible), cuya inclusión en el texto constitucional se justifica, sin embargo, por el propósito de ampliar al máximo el conjunto de los legitimados para impugnar cualquier perturbación de la libre comunicación social", y continúa manifestando que "el derecho a la información es, como los restantes derechos reconocidos en el arto 20, un derecho de libertad frente al poder y un derecho común a todos los ciudadanos".

Por ello creemos muy acertada la utilización del concepto más amplio de derecho a la libre comunicación pública que utiliza Torres del Moral[47], puesto que el objeto tanto del derecho a la información, como de la libertad de información es el mismo, proteger la libre comunicación o transmisión de informaciones; solo que, en un caso, esa libre comunicación de informacio-

---

[46] SALVADOR MARTÍNEZ, M: "El derecho a la información: una asignatura pendiente", en la obra colectiva de M.A. García Herrera (ed.), *Constitución y Democracia. 25 años de Constitución democrática en España*, Editorial: CEPC-Servicio Editorial de la Universidad del País Vasco, Bilbao, 2006, páginas 545 a 557.

[47] TORRES DEL MORAL, A: *Principios de Derecho Constitucional español*. 6º Ed. Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense. Madrid 2010, pág. 435.

nes se protege desde el punto de vista del emisor (libertad de información) y, en el otro, desde el punto de vista del receptor (derecho a la información). Como sigue manifestando el autor que venimos citando, "La libertad de comunicación pública, que ha tenido tradicionalmente y sigue teniendo una naturaleza *esencialmente negativa*, de rechazo de injerencias externas, se adorna en la actualidad de ciertos ribetes positivos porque demanda la actuación de los poderes públicos para la ordenación de los medios de comunicación que sirven de soporte material a dicha libertad. Este enfoque está expresamente asumido por el art. 20.3 de la Constitución en relación con los medios de titularidad pública, pero, a mi juicio, es extensible a otros, principalmente en el ámbito de la radiodifusión y de la televisión". Acertadamente continúa manifestando el autor que venimos citando, que: "La libertad de comunicación pública convierte a las personas en ciudadanos activos que compiten en el mercado ideológico, de modo similar a como lo hacen en el mercado económico, para defender sus ideas e intereses. Esta comunicación libre ayuda a que los grupos tomen conciencia de sus intereses y de sus posibilidades de satisfacción en el sistema político"[48].

Otro aspecto importante delimitado por la jurisprudencia del Tribunal Constitucional en la diferenciación entre libertad de información y expresión se concreta en los límites. Como manifiesta Salvador Martínez, "La diferenciación que el Tribunal Constitucional realiza entre la libertad de expresión y la de información tiene como consecuencia la existencia de dos tipos de límites: en primer lugar, los límites generales y externos, entre los que se encuentran los referidos a los derechos de la personalidad (arts. 20.4 y 18.1 de la Constitución), que afectan tanto a la libertad de expresión como a la libertad de información; y, en segundo lugar, dos límites específicos e internos, la veracidad y el interés público, cuyo respeto se exige exclusivamente para el legítimo ejercicio de la libertad de información. Así pues, de acuerdo con la interpretación de nuestro Tribunal Constitucional, la libertad de información no protege la transmisión de cualquier tipo de informaciones, sino sólo aquellas que respeten los requisitos de veracidad e interés público. Han de concurrir, pues, estos dos requisitos: que se trate de difundir información sobre un hecho noticioso o noticiable, por su interés público, y que la información sobre tal hecho sea veraz. En ausencia de alguno de estos dos requisitos la libertad de información no está constitucionalmente respaldada y, por ende, su ejercicio podrá afectar, lesionándolo, a alguno de los derechos que como límite enuncia el art. 20.4 CE"[49]. Como consecuencia de esta argumentación jurídica, en nuestro ordenamiento la diferenciación o delimitación entre libertad de expresión y la libertad de información es relevante en la práctica, solo para solventar el choque entre estas libertades y los derechos de la personalidad (honor, intimidad y propia imagen). De

[48] *Ibidem*, pág. 436.

[49] Obra citada, pág. 550 y 551.

esta forma, "en los casos en que se produzca una colisión entre los citados derechos, es preciso, de acuerdo con la jurisprudencia constitucional, determinar si estamos ante el ejercicio de la libertad de expresión o de la libertad de información, pues, para que el ejercicio de la libertad de información sea legítimo, es preciso que se respeten los dos citados límites internos (veracidad y relevancia pública), que no rigen sin embargo para el ejercicio de la libertad de expresión. Por el contrario, en los casos en los que no se produzcan este tipo de colisiones resulta irrelevante si el contenido del mensaje son opiniones o hechos; en estos casos el Tribunal Constitucional se refiere conjuntamente a «las libertades de expresión e información» sin distinguir entre una y otra, de modo que la estructura y el contenido de la libertad que el ciudadano ejerce, los obligados por ese derecho, los límites generales, las garantías específicas y la posible suspensión del derecho son iguales, tanto si se expresan opiniones, como si se divulgan hechos"[50].

También es relevante, que nuestro Tribunal Constitucional ha otorgado secularmente una posición preferente de la libertad de información respecto de los límites establecidos en el art. 20.4 CE, y se argumenta para ello que "… dada su función institucional, cuando se produzca una colisión de la libertad de información con el derecho a la intimidad y al honor, aquélla goza, en general, de una posición preferente, y las restricciones que de dicho conflicto puedan derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional, desnaturalizado ni incorrectamente relativizado". No obstante, esta prevalencia se condiciona a la ponderación de las circunstancias concretas de cada conflicto, y en todo caso habrá de determinarse, como requisitos para considerar legítimo el ejercicio de la libertad de información, la veracidad de la información difundida y el interés público de la misma.

El entramado jurídico expuesto, obedece a unos medios de comunicación que en la actualidad han variado de forma muy significativa. Como manifiesta Pauner Chulvi, "Debe reconocerse que las nuevas tecnologías han permitido la concurrencia de numerosos instrumentos alternativos a los medios «clásicos» de difusión de la información y hoy en día la web está dominada por contenidos generados por los usuarios, reconvertidos en los principales actores de la comunicación del siglo XXI, y por información compartida, vista y recibida por no profesionales. En este contexto, resulta más difícil reconocer qué elementos caracterizan el ejercicio profesional e incluso puede no resultar unívoco definir la misma profesión periodística … Entendemos, sin embargo, que estas actividades de difusión de información personal a través de las redes sociales no deben quedar exentas con carácter general de los principios en materia de protección de datos, habida cuenta

[50] *Ibidem*, pág. 552.

de los cada vez más invasivos modos en los que la información personal se maneja y difunde públicamente en las redes sociales"[51].

Hoy existen una multiplicidad de los conocidos como generadores de contenidos, que ya, y cada vez menos, tienen una referencia con los medios de comunicación clásicos (prensa, radio y televisión). Además de ello la información fluye en todos los sentidos, y no como lo hacía tradicionalmente. El mundo de la información y la comunicación ha variado de forma ostensible, y continuará haciéndolo. Como nos recuerda Pariser "El coste de producir y distribuir medios de comunicación de todo tipo -palabras, imágenes, videos y audio vía *streaming*- continuará cayendo, acercándose cada vez más a cero. A raíz de ello recibiremos un aluvión de opciones a las que prestar atención y seguiremos sufriendo de <<crisis de atención>>. Los gestores, ya sean humanos o software, serán más importantes que nunca y nuestra dependencia con respecto a esto a la hora de determinar qué noticias debemos consumir aún más creciente. Los redactores profesionales humanos son caros, mientras que codificar es barato. Dependemos cada vez más de una combinación de redactores no profesionales (nuestros amigos y colegas) y códigos informáticos para decidir qué mirar, leer y ver. Este código recurrirá al poder de la personalización y desplazará a los redactores profesionales humanos"[52]. Si a ello le añadimos que no existe en nuestro país ningún grupo de comunicación, o medio individualmente considerado, que sea económicamente sostenible con sus propios ingresos, parece claro que el panorama variará radicalmente en no mucho tiempo.

Pero todas estas novedades no suponen que tengamos que eliminar de nuestro ordenamiento jurídico las argumentaciones doctrinales y jurisprudenciales al respecto de esta materia, pero sí es obvio que requieren reinterpretaciones y actualizaciones, dado que las necesidades han variado de forma muy significativa[53].

En la Unión Europea no faltan pronunciamientos judiciales que suponen el inicio de argumentos jurídicos de cómo solventar las nuevas necesidades normativas. Los reconocimientos son bastantes coincidentes y podríamos agruparlos bajo un denominador común, prácticamente todos son de corte clásico. La Carta de Derechos Fundamentales de la UE, reconoce en su art. 11 la Libertad de expresión y de información con el siguiente texto:

> "1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar in-

---

[51] PAUNER CHULVI, C: "La libertad de información como límite al derecho a la protección de datos personales: La excepción periodística". En Teoría y Realidad Constitucional, UNED, núm. 36 de 2015, pág. 383.

[52] Obra citada, pág. 59.

[53] En el mismo sentido es interesante la opinión de PRESNO LINERA, M. A: Derechos fundamentales e inteligencia artificial. Marcial Pons. 2022, páginas 52 a 60.

formaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

2. Se respetan la libertad de los medios de comunicación y su pluralismo.

Por su parte, el CEDH, en su art. 10 y bajo el título de libertad de expresión establece que:

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial".

El RGPD hace excepción de la vigencia del derecho a la protección de datos de carácter personal con respecto a las denominadas informaciones periodísticas. De forma concreta el art. 85, bajo el título de Tratamiento y libertad de expresión y de información, establece que:

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

El Considerando 153 del texto que venimos analizando, concreta algo más, al establecer que "El tratamiento de datos personales con fines exclusi-

vamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio." Conviene recordar que la Ley Orgánica 3/2018 no concreta nada al respecto de esta materia.

Algo más clarificadora ha sido la jurisprudencia del TJUE al respecto de la materia. El Tribunal se pronuncia en el asunto Buivids[54] acerca de la aplicación de las limitaciones previstas en la normativa de protección de datos, cuando se difunden, a través de una plataforma de Internet, imágenes de otras personas grabadas por un usuario, y en concreto, si esta actividad puede constituir un tratamiento de datos personales con fines periodísticos.

Los hechos que originaron el presente litigio son los que se describen a continuación. El señor Buivids grabó en vídeo, en los locales de una comisaría letona, su propia declaración. El video, en el que aparecían varios policías en el ejercicio de sus funciones, fue publicado por el señor Buivids en la plataforma www.youtube.com sin el consentimiento de los policías. En este contexto, la Autoridad de control de Protección de Datos letona consideró que el señor Buivids había infringido la normativa de protección de datos, al no haber informado sobre la finalidad del tratamiento a los policías y le requirió para que suprimiera el vídeo de la plataforma.

Tras ver desestimadas sus pretensiones en primera y segunda instancia, el señor Buivids recurre ante el Tribunal Supremo de Letonia, que a su plantea cuestiones prejudiciales ante el TJUE, que de forma concreta tratan de aclarar dos aspectos: en primer lugar, si la grabación de funcionarios policiales en el ejercicio de sus funciones y su posterior publicación en YouTube es una

[54] Asunto C-345/17. Sentencia del Tribunal de Justicia UE (Sala Segunda) de 14 de febrero de 2019.

actividad comprendida en la normativa de protección de datos; y en segundo lugar, si esta actividad puede entenderse como un tratamiento de datos personales con fines periodísticos.

En la respuesta a la primera cuestión prejudicial, el TJUE, de acuerdo con los precedentes jurisprudenciales al respecto, afirma que las imágenes de una persona grabadas por una cámara y su posterior publicación en una página de Internet constituyen un tratamiento de datos personales de acuerdo con la normativa (apartados 31 y 35 de la sentencia). Además, en la medida en que el señor Buivids publicó las imágenes sin restricciones de acceso, no puede considerarse que el tratamiento se realice en el marco de actividades exclusivamente personales o domésticas. Tampoco el hecho de que sean funcionarios públicos excluye, a juicio del TJUE, la aplicación de la normativa de protección de datos. Por tanto, la cuestión relevante se centra en concretar si el tratamiento de datos llevado a cabo por el señor Buivids constituye una actividad con fines periodísticos. En este sentido, el Tribunal confirma su jurisprudencia anterior de acuerdo con la cual, el termino periodismo no se limita a medios de comunicación profesionales, sino que incluye actividades que tienen por finalidad "divulgar al público información, opiniones o ideas por cualquier medio de transmisión" (apartado 53 de la sentencia).

Siendo así, una grabación como la controvertida, esto es, efectuada por una persona no periodista profesional y publicada en una plataforma de compartición de contenidos, puede constituir una actividad periodística. A juicio del TJUE, el tribunal remitente debe comprobar si la actividad controvertida tiene como única finalidad la divulgación al público de información, opiniones o ideas (apartado 59 de la sentencia).

Para realizar este análisis, el TJUE aporta ciertos criterios que deben ser tenidos en cuenta: que la actividad contribuya a crear un debate de interés general; el objeto del reportaje; el comportamiento anterior del interesado; el contenido; la forma y las repercusiones de la publicación; la forma y las circunstancias en que se obtuvo la información; su veracidad; y las medidas adoptadas para mitigar el alcance de la injerencia en el derecho de la intimidad.

La sentencia tiene especial importancia porque delimita la interpretación que debe realizarse de la excepción "con fines periodísticos", que debe incluir a periodistas no profesionales, como pueden ser blogueros o usuarios, así como los conocidos de forma genérica como generadores de contenidos, es decir, cualquier persona.

La libre comunicación es, inexorablemente, otro de los pilares de nuestra ordenación social, clave en la conformación ideológica del ciudadano, esencial en un aspecto de la libertad, necesario para el pluralismo social, y elemento estructural básico de los sistemas democráticos. Existe una lectura quizás más clarificadora en sentido negativo, de tal forma que en la medida que se limita, manipula o condiciona la libertad de comunicación pública, el individuo es menos libre y la sociedad en la que se integra, menos demo-

crática, y el tratamiento masivo de datos, y el uso de la Inteligencia artificial, ofrecen la posibilidad, bastante accesible, de limitar, manipular, o condicionar la libre comunicación, a la vez que generalizar la desinformación o confusión informativa. Se constituyen en una clara amenaza al derecho objeto de estudio, y la normativa y la construcción jurídica existente son insuficientes para hacerle frente. La jurisprudencia, al igual que la legislación, no conforman la realidad con carácter absoluto. La primera resuelve un conflicto jurídico, normalmente interpretativo o aplicativo; la segunda tiene una pretensión ordenadora en base a un fin, pero no garantiza tampoco la consecución total del mismo. Ambos son mecanismos de eficacia parcial e independientes de otros muchos elementos. Son herramientas necesarias, pero insuficientes, y en el ámbito que nos ocupa, queda evidente su eficacia parcial. Se requieren nuevos mecanismos jurídicos.

Aunque en el apartado final de este trabajo se exponen una amplitud de soluciones y propuestas, cabe adelantar aquí, que la primera medida para paliar esta situación es la transparencia en el uso de los algoritmos que producen y tratan la información, así como también de aquellos que la seleccionan o reorientan. El algoritmo se constituye en una potente herramienta al servicio del poder, en su más amplio sentido de la expresión, de intereses concretos, y opera de forma oculta, sin posibilidad de contrapeso, de límite o de mecanismo de reequilibrio. La ausencia de conocimiento de su uso, o de la transparencia en su utilización lo convierten en un medio de manipulación de información, y singularmente de los medios a través de los que esta se transfiere. Esta circunstancia nos hace retrotraernos varios siglos atrás en nuestra conformación social.

Más allá de las necesidades jurisprudencial, legislativas y doctrinales, el ciudadano también debe irse acomodando a ciertas circunstancias novedosas. Durante mucho tiempo se ha atenido a lo escrito, visto y oído como realidades inmutables, como verdades absolutas. Esta circunstancia debe ir variando, el ciudadano debe asumir que todo lo que se escribe, se ve u oye, tiene un variable grado de coincidencia con la realidad que puede cuantificarse numéricamente. Interiorizar esta técnica de filtrado de la información debe constituir en la actualidad una práctica habitual, a la que indefectiblemente ayuda el conocimiento de su proceso de elaboración, o la transparencia en su generación. Nuevas circunstancias deben generar nuevos hábitos, es la materialización del efecto acción-reacción, tan propio de la condición humana.

6. Derecho a la igualdad

Como nos recuerda Gómez Sánchez[55], el principio de igual está inexorablemente unido al surgimiento del Estado de Derecho, y aunque existe una

[55] GÓMEZ SÁNCHEZ, Y: *Constitucionalismo Multinivel. Derechos Fundamentales.* 4ª Ed. UNED y Sanz y Torres. Madrid 2018, páginas 283 y 284.

primera aportación del Estado liberal, su surgimiento y plasmación jurídica devendrá con el surgimiento del Estado social, de tal forma que "La población ya no demandaba la abstención del Estado y el libre desenvolvimiento de la sociedad civil, sino que ahora solicitaba servicios y prestaciones públicas. Pero este nuevo Estado interventor transforma también el principio de igualdad. Esta transformación se opera cuando se abandona en parte la concepción de la igualdad como un punto de partida y se defiende, sin embargo, la igualdad como una finalidad y sobre todo como un instrumento de transformación social, lo cual, por otro lado, era uno de los postulados principales del Estado social. Podríamos, incluso, enunciar la tesis de manera más radical ya que el Estado liberal no podía crear una sociedad en la que la igualdad primaria, pues ello hubiera resultado incompatible con sus principios estructurales. Sólo en un Estado social que propugna la redistribución y la nivelación social se podía defender un principio de igualdad que se superponga a las desigualdades naturales. ... Será el constitucionalismo posterior a la Segunda Guerra Mundial (que también extenderá la implantación de la justicia constitucional), el que definitivamente incorpore esta nueva versión del principio de igualdad que ahora emerge como una *igualdad material* (también denominada *real*, *efectiva* o de *oportunidades*) que a partir de entonces coexiste con el más tradicional principio de *igualdad formal*, en sus manifestaciones de *igualdad ante la ley* e *igualdad en la ley*." Este concepto jurídico de igualdad no ha dejado de ampliarse y concretarse en los ordenamientos jurídicos modernos, alcanzado prácticamente a todos los ámbitos de la vida social, y con sus respectivos traslados al ámbito jurídico, y también a la sociedad digital de forma muy pareja y coetánea en tiempo.

Puede afirmarse que la concreción del derecho fundamental a la igualdad tiene su plasmación en el contexto de la sociedad digital, en dos formulaciones esenciales, la Red neutral y el principio de acceso universal a la Red, aspectos que analizamos por separado a continuación.

6.1. Red Neutral

Internet es el mayor y mejor instrumento de cambio social conocido en la era de la humanidad. No hay ninguna otra creación humana parangonable con ello, y afortunadamente se ha conseguido sin menoscabo de vidas humanas, es el producto del desarrollo humano y de las capacidades del hombre. Hoy se ha convertido en algo consustancial al ser humano y a la organización social, a la vez que se constituye en el mecanismo de máxima proyección para el ser humano. El estudio de su conformación y regulación se ha instituido en una parte esencial del Derecho, y no sólo nacional, sino también internacional.

Existe al respecto de la Red y el Derecho una concepción de espacio de libertad, este trasfondo es el que acuña el concepto de Red como *ciberlibertaria*, y que encuentra sus orígenes en la Declaración de Independencia del

Ciberespacio. Parte de la idea de que la Red no es propiamente un sujeto material, por lo cual debe ser ajeno a la influencia de poderes políticos y también del Derecho. El ciberespacio sería así una realidad inmaterial, únicamente regulada por la voluntad de sus partícipes (autorregulación). Ello tiene un fuerte componente imaginario e ilusorio, próximo a un mundo virtual eternamente feliz. Esta concepción de Internet y también del Metaverso, que podría tener cierto encuadre en 1996, ahora está muy lejos de la realidad, pero curiosamente, está muy presente y es objetivo esencial de muchos sectores ideológicos y políticos. Pero es irrealizable, si bien no teóricamente, sí en la práctica. Por mucho que se quiera configurar un mundo distinto en el ciberespacio, la persona es parte integrante de él, y la persona y sus relaciones sociales son las que determinan su conformación. El hombre cuando se inserta en el mundo virtual no queda desposeído de sus características o condicionamientos, la condición humana no se filtra, de tal modo que desparezcan todos los elementos negativos inherentes a él. De esta forma, lo relevante no es el contexto, el mundo que conformamos, sea real o virtual, lo determinante son las personas. Hace 10.000 años los medios para cometer delitos eran muy precarios, pero se cometían. Hoy siguen existiendo delitos, injusticias y muchos desequilibrios, y la necesidad de que la sociedad establezca soluciones a ellos. Poco hay de nuevo en las relaciones personales y sociales, y en la condición humana. Las personas siguen siendo violentas o pacíficas, egoístas o humanitarias, racionales o irracionales, sigue existiendo el robo, el crimen, la violencia, la pobreza, la marginación y la violación de derechos fundamentales, a pesar de que ha variado de forma muy considerable el contexto humano. Los avances tecnológicos no despojan al ser humano de sus características innatas, al igual que tampoco desmontan las relaciones sociales. En un mundo virtual, si hay humanos habrá bondad y maldad, habrá solidaridad y egoísmo, habrá amor y odio, habrá libertad y sometimiento, y habrá también violencia y concordia. En definitiva, existirá, al igual que en el mundo real, lo que es innato al ser humano. Por ello, las relaciones humanas requieren de normas para ordenar la convivencia, y se requiere del poder político como contrapeso necesario y como garante del bien común o del interés general.

Internet necesita de los mecanismos clásicos de la ordenación social, a la cabeza de los cuales se encuentra el Derecho. Es utópico o ilusorio entender a la Red como un ámbito exento de regulación jurídica, sería tanto como volver a las primeras formas de organización social, donde el más fuerte o la teocracia, en sus distintas vertientes, eran las formas de ordenación, o en todo caso es una forma de asegurar la anarquía más absoluta, y como ocurre ahora con el mundo *Woke* en las redes sociales, a la arbitrariedad y sometimiento más puro de los usuarios.

El problema ahora no es si la Red debe estar sometida y regulada por el Derecho, circunstancia ésta indiscutible, la cuestión es cómo se articula ese Derecho y qué vigencia tiene. La primera gran dificultad proviene de un

límite propio de aquél, que tiene una radicación estatal, donde la vigencia de las normas coincide con la extensión territorial del Estado. Pero la Red no tiene fronteras, ni físicas, ni temporales, por lo que se introduce la necesidad de regulación jurídica. Para solventar este conflicto han sido muy útiles las regulaciones supraestatales o regionales, como ocurre con el Consejo de Europa y la Unión Europea, pero se adolece de una normativa efectiva de carácter internacional. Constatada la realidad expuesta, no es menos cierto que al respecto de la Red se vienen aplicando determinados principios que en gran medida tienen carácter universal. Quizás el de más amplio reconocimiento sea el de la necesidad de una Red neutral.

El principio de neutralidad de Red establece que la información sea transmitida sin discriminación, esto es, que sea tratada con igualdad, independientemente de su naturaleza, origen, destino, o cualquier otra circunstancia. El término neutralidad de la Red lo acuñó Tim Wu, en 2003, y se constituye hoy en uno de elementos centrales para la comprensión de la relación entre Derecho e Internet.

Hablar de neutralidad de la Red es hablar de uno de los principios fundamentales para el funcionamiento de Internet. Según este principio, toda la información o dato que circule por la Red debe ser tratado de la misma forma y sin importar quien lo emite o quien lo vaya a recibir. Este principio suele chocar frontalmente con los intereses comerciales. Las grandes empresas, como Google, consideran que sus datos son más valiosos, en tanto tienen más demanda, por lo que deberían ser tratados con preferencia y así mejorar sus servicios. Al igual que este criterio, surgen otros muchos que postulan o justifican una intervención o discriminación en el tránsito de los datos por la Red. Desde los orígenes de la Red, se ha sido consciente de que los ciudadanos y las empresas tienen derecho a que el tráfico de datos recibido o generado no sea manipulado, tergiversado, impedido, desviado, priorizado o retrasado en función del tipo de contenido, del protocolo o aplicación utilizado, del origen o destino de la comunicación, ni de cualquier otra consideración ajena a la de su propia voluntad. Junto a ello, no debemos olvidar que proteger la neutralidad de la red supone también proteger otros derechos fundamentales de los ciudadanos.

En 2005, la FCC de Estados Unidos (*Federal Communications Commission*), estableció las cuatro libertades de Internet (acceso, uso, conexión de terminales y competencia), añadiendo en 2007 dos libertades adicionales: transparencia y no discriminación. Estos son hoy los principios básicos que sustentan la conformación universal de la Red. Se cumplen en distinto grado dependiendo de los Estados y de las circunstancias concretas de cada país. No obstante, puede extraerse de forma pacífica la conclusión de que a mayor nivel de desarrollo económico y democrático, más y mejor se cumplen los principios enunciados.

Aunque la neutralidad de la Red sea un principio fundamental de Internet y debería considerarse como uno de los derechos fundamentales de los ciudadanos en la misma, lo cierto es que no son pocas las prácticas destinadas a alterarla. Consciente de esta realidad, el Parlamento Europeo, en noviembre de 2017 aprueba la Resolución *The open internet and net neutrality in Europe*, con objeto de que se vaya conformando una normativa que evite la intervención en la Red que suponga discriminación en el tráfico y tratamiento de los datos.

En principio, y de forma muy genérica, puede utilizarse la definición de Red neutral como aquella que permite comunicación de punto a punto sin alterar su contenido. También puede delimitarse de forma sencilla utilizando el principio en virtud del cual, los proveedores de servicios de Internet y los gobiernos que la regulan, deben tratar todo tráfico de datos que transitan por la Red de igual forma, sin aplicar criterios que puedan afectar al contenido, o a los medios usados.

A ello hemos de añadir que la neutralidad de la Red comprende dos compromisos de no discriminación diferentes: uno de servicio universal; y otro de servicio público de transporte. El primero es la llamada neutralidad de la *red lite*, que mira hacia el pasado y que reivindica que los usuarios de Internet no deberían estar en desventaja por las prácticas de los proveedores de Internet. El argumento es que se debe prestar un nivel mínimo de servicio que ofrezca acceso abierto a Internet sin bloquear o degradar aplicaciones o protocolos específicos, lo que se ha descrito como una versión actualizada del servicio universal y que en general se propone a 2 Mbps. Esto proporciona un nivel básico de servicio que en último término todos los abonados deberían recibir. La llamada neutralidad de la *red positiva*, con vistas al futuro, describe una práctica según la cual la oferta de una mayor calidad de servicio a precios más altos debe realizarse en condiciones justas, razonables y no discriminatorias a todos los interesados, lo que supone un equivalente moderno del servicio público o *common carriage*. Se trata de un principio más discutible, y muchos proveedores de contenidos y operadores establecen sus políticas de mercado, a lo que no puede oponerse ninguna objeción desde la perspectiva jurídica. Como el principio de servicio público o *common carriage*, dicta los términos, pero no las condiciones específicas del mercado, la transparencia y la no discriminación no se traducirían automáticamente en una pluralidad de servicios. Como puede comprobarse, la regulación de la Red es una cuestión compleja, en la que intervienen una multiplicidad de factores y donde los eslóganes o conclusiones fáciles son pura demagogia o defensa de un interés particular.

La primera y más clara deducción que hemos de obtener al respecto de la Red es su necesidad de regulación jurídica, a la que se suma la intervención de los poderes públicos, con objeto de garantizar su finalidad social. Indefectiblemente estas dos aportaciones deben tener un carácter supranacional, o de forma más concreta, la normativa debe tener ámbito universal.

Las normas del Estado, y su poder político, son ahora inertes ante la revolución que supone el uso de la Red, y obligan a una regulación de carácter universal. De igual forma, y como venimos argumentado, debe ser prioridad del Estado, garantizar el acceso a Internet sin que exista desigualdad o diferenciación alguna, ya sea de carácter social, económico, técnico, cultural o de otra índole. El principio de igualdad como elemento básico del Estado social, se debe traducir en el ámbito de la sociedad digital en la pretensión de la mayor libertad posible, a la vez que compaginado con el principio de igualdad, o en su vertiente negativa, de no discriminación de acceso o de tránsito de contenidos. Esta tarea no se plantea como sencilla, máxime en un mundo tan mercantilizado y basado en el consumo, como es el actual, pero en todo caso, es tarea inexcusable del Estado garantizar este derecho.

El papel que juega la IA respecto de la Red neutral es capital. La posibilidad de filtrar, distorsionar, modificar, sesgar o limitar contenidos, en definitiva, de discriminar en función de los sujetos, es algo cotidiano en ámbitos como la información, la actividad comercial, política y de forma más genérica, social.

En el mismo momento en que pasamos del ámbito estatal al universal en los postulados de la Red neutra, nos encontramos con un enorme problema, y al que ya hemos hecho referencia. La división del mundo en dos grandes bloques, países democráticos y regímenes autocráticos, al que se suman los posicionamientos geoestratégicos y geopolíticos, descomponen la sencillez de las propuestas de solución. Varían por completo las pretensiones, y por tanto, las posibilidades de implantación con carácter universal. Existen dos mundos contrapuestos, pero que no son desconocidos el uno del otro, a la vez que no son permeables, más bien al contrario, se repelen e intentan neutralizarse. De esta forma los países y entornos autocráticos usan la Red como elemento de control, y sus actuaciones están muy alejadas de un espacio de libertad y menos aún, poseen una justificación en la igualdad. Obedecen en esencia a intereses de poder, a pretensiones ideológicas, muy alejadas de los principios en los que se sustentan las ordenaciones sociales de los países occidentales, en los cuales es frecuente perder la perspectiva universal, y olvidar la máxima de que vivimos en un mismo mundo, en el que hay muchas realidades. Pero no debemos ser ilusos, la Red es una potentísima herramienta de poder político, económico, cultural, social, un gran espacio de libertad, y de igual forma, de control y sometimiento, y esto es aplicable a los dos mundos que hemos referido, el occidental y democrático, y el autocrático. La neutralidad de la Red debe ser una aspiración, pero no es una realidad, ni en los países democráticos, ni en los autocráticos. Lo cual no es óbice para puntualizar las grandes diferencias que se dan entre uno y otro mundo. En los países democráticos la Red presenta unas características de sometimiento o control a intereses comerciales, de grupos de presión o de interés, y precisamente por tener un menor control ideológico, también a la injerencia difusa de los regímenes autocráticos. Por el contrario, en los paí-

ses carentes de democracia, y aunque no desconocedores de dicho mundo, la neutralidad de la Red se ve perturbada por la ideología o por los fines políticos, y se justifica, curiosamente, en el objetivo del beneficio social, incluso en muchas ocasiones en la propia igualdad. Rusia, China o Irán son claros ejemplos de esta tesitura.

6.2. El acceso universal a internet

Frank La Rue, relator especial sobre promoción y protección del derecho de libertad de expresión, presentó un informe a la Asamblea General de la ONU en el que recomendó consolidar el acceso a Internet como derecho fundamental. Manifiesta que dado el poder especial que le confería su carácter interactivo, Internet debería considerarse un elemento necesario para el ejercicio de muchos derechos en la esfera socioeconómica y para la promoción de la diversidad cultural en el mundo. Con dicho informe comenzó a gestarse el desarrollo del acceso a Internet como derecho fundamental. La resolución fue aprobada recientemente, aunque contó con el rechazo de países como Rusia, China, Arabia Saudita, Sudáfrica e India, quienes mostraron dudas respecto de la conveniencia de la redacción final del texto. Hay que tener en cuenta que en dichos países son frecuentes las limitaciones parciales o temporales de acceso a la Red, a la vez que no tienen un concepto de derechos fundamentales homologable a países democráticos.

La resolución aboga por garantizar el acceso a Internet, ya que "facilita vastas oportunidades para una educación asequible e inclusiva a nivel mundial", o proporciona otros recursos para la educación, y en especial pretende evitar la brecha digital. De forma concreta se establece que se "Exhorta a todos los Estados a que consideren la posibilidad de formular, mediante procesos transparentes e inclusivos con la participación de todos los interesados, y adoptar políticas públicas nacionales relativas a Internet que tengan como objetivo básico el acceso y disfrute universal de los derechos humanos".

Como bien conocemos, esta normativa no tiene vinculación jurídica, si bien supone un punto de inicio para que los Estados regulen la materia y una aspiración próxima de los países menos desarrollados. Pero el problema esencial al respecto del acceso universal se plantea en la doctrina en referencia a si debe o no clasificarse como un derecho fundamental, es decir en igual necesidad de protección a los ya incluidos en esta categoría máxima de garantía.

El primer elemento que debemos clarificar es el de considerar si el acceso a Internet es en realidad un derecho, y además un derecho fundamental (derecho humano en la terminología anglosajona). Para Vinton Cerf, inventor del protocolo TCP/IP y uno de los padres de Internet, en ocasiones estamos pasando por alto el punto más importante: la tecnología es un facilitador de los derechos, no un derecho en sí, por ello es un error colocar

cualquier tecnología en esta máxima categoría, ya que con el tiempo terminaremos valorando las cosas equivocadas. Según Cerf para que algo tenga consideración de derecho humano debemos tener más altura de miras. Un derecho básico debe ser una de las cosas que, como seres humanos, necesitamos para llevar vidas saludables y significativas, como la libertad, la condena de la tortura o la libertad de conciencia. Es un error colocar cualquier tecnología en esta máxima categoría. Cerf pone un ejemplo muy clarificador: hace tiempo, si no tenías un caballo era difícil ganarse la vida. Pero el derecho importante en ese caso era el derecho a ganarse la vida, no el derecho a un caballo. De la misma manera, ningún país decretó nunca que todo el mundo tuviera derecho a un teléfono. El padre de Internet considera que el teléfono nos acercó a la noción de servicio universal (en el que también está la electricidad y, por qué no, una conexión a Internet de banda ancha), pero que no debemos confundir servicio universal con derecho humano.

Los avances científicos y tecnológicos presentes en un mundo globalizado como el que caracteriza nuestra sociedad actual tienen, de forma clara y directa, impacto en los derechos fundamentales. El surgimiento de nuevas tecnologías, como Internet, han cambiado el ejercicio de derechos como el acceso a la información, libertad de asociación, libertad de expresión y pensamiento, el derecho a la educación, la salud, pero a la vez han incidido o hecho más vulnerables otros derechos, como el derecho a la seguridad, la intimidad, la libertad ideológica, la igualdad, la libertad de expresión e información, entre otros. Las nuevas tecnologías no solo producen bienestar o comodidad, también libertad y facilidad para el ejercicio de derechos y libertades fundamentales.

Como indica Miranda[56] el derecho de acceso a internet "debe considerarse un derecho social, o más bien una pretensión subjetiva que debe ser satisfecha con prestaciones públicas, al igual que el derecho a la educación, de la salud y la prevención social. Un servicio universal que las instituciones nacionales deben garantizar a sus ciudadanos a través de inversiones estatales, y políticas sociales y educativas. En efecto, cada vez más el acceso a la red de internet, y el desarrollo de esa actividad, constituye el modo en el cual el sujeto se relaciona con los poderes públicos, y por lo tanto, ejerce sus derechos. El uso de internet se está convirtiendo en una herramienta imprescindible para la libertad de expresión y para el acceso a la información. Más que una posibilidad de comunicación se está convirtiendo en una necesidad debido al periodo de globalización que hoy se vive. En este sentido, los Estados tienen la obligación de promover el acceso universal a internet para garantizar el disfrute efectivo del derecho a la libertad de expresión. El acceso a internet también es necesario para asegurar el respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo,

[56] MIRANDA BONILLA, H: "El acceso a internet como derecho fundamental". En Revista Jurídica IUS Doctrina nº 15 de 2016, pág. 9 y ss.

el derecho de reunión y asociación, y el derecho a elecciones libres". Esta argumentación doctrinal del derecho de acceso a internet como derecho humano, fundamental o constitucional, ha tenido su fundamentación esencialmente en Italia[57], en Hispanoamérica[58], y también en Alemania[59], y se viene asentando doctrinalmente en el sustrato ya consolidado del derecho a la igualdad, y singularmente a la igualdad de oportunidades. Si Internet es ya, y lo será en un futuro inmediato cada vez más, el motor del desarrollo social, no existe la menor duda de que hay una correlación esencial con el derecho a la igualdad, de igual forma que ocurriera en siglos pasados con la educación o el acceso a la cultura, como elemento de dinamización social y desarrollo individual. En igual grado en que el ciudadano se aleja del desarrollo tecnológico, se distancia de la necesaria integración social.

La importancia del acceso a internet como forma de eliminar la desigualdad se ha plasmado en la normativa, y de forma concreta, la LO 3/2018, en su art. 97, relativo a "Políticas de impulso de los derechos digitales", por parte de los poderes públicos, se obliga al Gobierno, en colaboración con las CC. AA., a elaborar un "Plan de Acceso a Internet", con tres objetivos fundamentales:

a) superar las brechas digitales, garantizando la accesibilidad a Internet de colectivos vulnerables o con necesidades especiales, mediante medidas como un bono social de acceso a Internet;

b) impulsar la existencia de espacios públicos para la conexión a Internet;

c) fomentar la formación en competencias y habilidades digitales básicas, así como la capacidad de todas las personas para realizar un uso autónomo y responsable de las tecnologías digitales, mediante medidas educativas.

Por otra parte, prevé la aprobación de un Plan de Actuación enfocado a promover acciones de formación, difusión y concienciación para un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales por parte de los menores, a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y derechos fundamentales.

Como nos recuerda Zapatero Martín[60], en el seno de la Asamblea General de las Naciones Unidas, se ha aprobado la Agenda 2030 para el Desarrollo

---

[57] Entre otros, FROSINI, V: *Cibernética, Derecho, Internet y sociedad*. Lex-Olejnik. Santiago de Chile. 2019; RODOTÁ, S: *La vida y las reglas*. Trotta. 2010.

[58] Obra citada de Miranda Bonilla.

[59] Por todos HOFFMANN-RIEM, W: *Big Data. Desafíos también para el Derecho*. Traducción de López Pina. Cívitas Thomson-Reuters. Madrid 2018.

[60] En REBOLLO DELGADO, L y ZAPATERO MARTÍN, P: *Derechos Digitales*. Dykinson, Madrid 2019, páginas 207 y ss.

Sostenible que, en su Objetivo 9[61], contempla la construcción de infraestructuras resilientes, la promoción de la industrialización inclusiva y sostenible, así como el fomento de la innovación. Una de las metas planteadas es el aumento significativo del acceso a la tecnología de la información y las comunicaciones, a fin de proporcionar acceso universal y asequible a Internet en los países menos adelantados antes de 2020. Por otra parte, su "Objetivo 4[62]", se centra en garantizar una educación inclusiva, equitativa y de calidad, promoviendo oportunidades de aprendizaje para todos. Se reconoce que la educación es la base para mejorar la calidad de vida y, especialmente, "el acceso a la educación inclusiva y equitativa puede ayudar a abastecer a la población local con las herramientas necesarias para desarrollar soluciones innovadoras a los problemas más grandes del mundo".

Por su parte, en el ámbito de la UE, se ha adoptado una Agenda Digital para Europa[63], cuya principal finalidad es el establecimiento de un mercado único digital, basado en una Internet rápida en aplicaciones interoperables. La Agenda pretende fomentar la innovación, el crecimiento económico y la mejora de la vida cotidiana tanto para los ciudadanos como para las empresas. En el citado documento, se reconoce la existencia de carencias en la alfabetización y capacitación digitales, que llevan a producir la exclusión de muchos ciudadanos de la sociedad y la economía digitales, por lo que resulta necesaria una reacción coordinada de los Estados miembros para garantizar que los ciudadanos puedan acceder a los servicios de Internet de modo muy rápido y a un precio competitivo. Con esta finalidad, se propone la elaboración de una política global, basada en una combinación de tecnologías, que se centre en dos objetivos: en primer lugar, garantizar la cobertura universal de la banda ancha, con velocidades de internet que vayan aumentando gradualmente hasta los 30 Mbps; en segundo lugar, con el tiempo, incrementar el despliegue de las redes de acceso de nueva generación (NGA) para hacer posibles conexiones ultrarrápidas en una gran parte del territorio de la UE.

En el marco de dicha política global, las autoridades competentes estarán obligadas a garantizar que las obras de ingeniería civil, públicas y privadas, tengan en cuenta las redes de banda ancha y el cableado dentro de los edificios, aplicando derechos de paso y cartografiando las infraestructuras pasivas disponibles adecuadas para el cableado. En definitiva, la política europea deberá fomentar una gestión eficiente del espectro de la radiodifusión, imponiendo la utilización de determinadas frecuencias del dividendo digital para la banda ancha inalámbrica, garantizando cierta flexibilidad y respetando la competencia y la innovación.

---

[61] https://www.un.org/sustainabledevelopment/es/infrastructure/

[62] https://www.un.org/sustainabledevelopment/es/education/

[63] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ES:PDF

Por último, conviene reseñar, que el Parlamento Europeo ha dictado un conjunto de mandatos sobre la materia, y de forma concreta, en la Resolución de 2017[64] incorpora un apartado de no discriminación en el que se pone de manifiesto lo siguiente:

> "19. Hace hincapié en que, como consecuencia de los conjuntos de datos y sistemas de algoritmos que se utilizan al hacer evaluaciones y predicciones en las distintas fases del tratamiento de datos, los macrodatos no solo pueden resultar en violaciones de los derechos fundamentales de los individuos sino, también, en un tratamiento diferenciado y en una discriminación indirecta de grupos de personas con características similares, en particular en lo que se refiere a la justicia e igualdad de oportunidades en relación con el acceso a la educación y al empleo, al contratar o evaluar a las personas o al determinar los nuevos hábitos de consumo de los usuarios de los medios sociales;
>
> 20. Insta a la Comisión, a los Estados miembros y a las autoridades encargadas de la protección de datos a que definan y adopten las medidas que se impongan para minimizar la discriminación y el sesgo algorítmico y a que desarrollen un marco ético común sólido para el tratamiento transparente de los datos personales y la toma de decisiones automatizada que sirva de guía para la utilización de los datos y la aplicación en curso del Derecho de la Unión;
>
> 21. Pide a la Comisión, a los Estados miembros y a las autoridades de protección de datos que evalúen de manera específica la necesidad, no solo de transparencia algorítmica, sino también de transparencia en relación con posibles sesgos en los datos de capacitación utilizados para hacer inferencias sobre la base de los macrodatos;
>
> 22. Recomienda que las empresas lleven a cabo evaluaciones periódicas sobre la representatividad de los conjuntos de datos, que consideren si los conjuntos de datos se ven afectados por elementos sesgados, y que desarrollen estrategias para superarlos; pone de relieve la necesidad de examinar la exactitud e importancia de las predicciones basadas en el análisis de los datos teniendo presente las preocupaciones de carácter ético y la equidad".

A nuestro juicio, tanto el concepto de red neutral, como el de acceso universal a internet, se constituyen en medios necesarios para hacer efectivo el derecho a la igualdad en un mundo globalizado. La cuestión doctrinal a dilucidar es si estos son derechos, o tienen carácter instrumental, o entidad suficiente para ser considerados derechos fundamentales, y lo más importante, cómo juega esta categorización en relación con la Inteligencia artificial y

---

[64] Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI).

el uso masivo de datos, o planteado desde otra perspectiva, se hace necesario dotarles de un mayor grado de protección frente a esta nueva amenaza.

La realidad es que hoy hay un conjunto enorme de ciudadanos ubicados en lo que se denomina la periferia digital, apátridas digitales, excluidos de la vigencia de uno de los principios organizadores de la sociedad básicos, como es el de la igualdad, y el acceso universal a Internet se constituye en una herramienta necesaria para paliarlo.

Si hemos de posicionarnos al respecto de las dos materias abordadas en este apartado, la Red neutral y el acceso universal a Internet, a mi juicio no se constituyen en un derecho fundamental, pero son determinantes para la vigencia del derecho fundamental a la igualdad, son para él un colaborador necesario, una herramienta esencial de inclusión y no discriminación. Es una corriente extendida hoy, incluso dentro de los estudiosos del Derecho, de elevar todo a la categoría de derecho fundamental. Se hace ello con el loable propósito de ofrecer un mayor nivel de garantía y de protección. Pero el jurista debe deslindar con claridad los propósitos de los medios, y en el ámbito de las nuevas tecnologías esta circunstancia se multiplica de forma exponencial, es probable que sea debido a la desnudez jurídica con que nacen. Pero esta circunstancia no nos debe hacer perder de vista lo sustantivo, lo esencial, lo *sine qua non*. En este grupo hay que incluir el derecho a la igualdad, pero no las formas de llevarlo a cabo o hacerlo efectivo. Pero ello no puede aminorar la importancia que las dos pretensiones que hemos analizado en este apartado tienen en la actualidad, y singularmente para alzar a un número enorme de personas al ámbito de lo digital, como elemento insoslayable de mejora en sus condiciones de vida, y de medio para conseguir la vigencia de la mayoría de los derechos fundamentales y, esencialmente, del derecho a la igualdad.