PRIVACIDAD Y DERECHOS DIGITALES[1]

Mónica Arenas Ramiro*
David Díaz Lima**

1 El presente Capítulo se ha elaborado en el marco del proyecto de investigación PID2021-128309NB-I00, cuyas investigadoras principales son las Profesoras Rosario García Mahamut y Beatriz Tomás Mallén.

* Profesora Contratada Doctora de Derecho Constitucional, Universidad de Alcalá.

** Profesor universitario, Abogado especializado en protección de datos personales.

I. INTRODUCCIÓN: LA DIGNIDAD DE LA PERSONA COMO PUNTO DE PARTIDA

En el proceso de digitalización que vivimos, el tratamiento de nuestra información personal se convierte en un elemento imprescindible tanto para el sector público como para el privado. Garantizar el poder de disposición de los datos personales, como parte integrante del derecho a la vida privada[2], se convierte igualmente en un requisito indispensable no sólo para los individuos, sino para los propios Estados[3].

El derecho a la protección de datos personales tiene un carácter transversal e instrumental a todos los derechos[4], especialmente en el entorno digital, donde lo que se mueve esencialmente es información personal o, incluso, donde sin llegar a ser información personal –requisito que exige el Reglamento General

2 STEDH de 16 de febrero de 2000, asunto Amann contra Suiza, § 65.

3 Recordamos aquí que la privacidad es un derecho reconocido en textos internacionales y europeos, como en la Declaración Universidad de Derechos Humanos (art. 12), en el Pacto Internacional de Derechos Civiles y Políticos (art. 17), en el art. 8 Convenio Europeo de Derechos Humanos, o, a nivel de la Unión Europea, en el art. 8 Carta de Derechos Fundamentales de la Unión Europea.

4 El derecho a la protección de datos se garantiza en el art. 18.4 CE, así como (entre otras normas) en el art. 8 Carta de Derechos Fundamentales de la Unión Europea y forma parte del contenido de la vida privada garantizado por el art. 8 Convenio Europeo de Derechos Humanos. En relación con su carácter instrumental, la STC 290/2000 lo reconoce como un instituto de garantía del resto de derechos fundamentales del ordenamiento jurídico y señala: "En lo que respecta al primer presupuesto, si el art. 1 L.O.R.T.A.D. establece que su objeto es el «desarrollo de lo previsto en el apartado 4 del art. 18 C.E.», es procedente recordar que este precepto, como ya ha declarado este Tribunal, contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que es, además, en sí mismo, «un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama 'la informática'» (STC 254/1993, de 20 de julio, F.J. 6, doctrina que se reitera en las SSTC 143/1994, de 9 de mayo, F.J. 7; 11/1998, de 13 de enero, F.J. 4; 94/1998, de 4 de mayo, F.J. 6, y 202/1999, de 8 de noviembre, F.J. 2)" (FJ 7º).

de Protección de Datos europeo (RGPD)[5] para poder ser de aplicación–[6], acaba afectando al desarrollo personal del sujeto.

Así las cosas, garantizando el derecho a la protección de datos personales, se garantiza el ejercicio del resto de derechos fundamentales y, por lo tanto, se garantiza el libre desarrollo personal. Debemos proteger nuestra privacidad, de la que forma parte el tratamiento de nuestros datos personales, sean íntimos o no[7], para garantizar nuestro libre desarrollo personal.

El principal problema al que nos enfrentamos es el hecho de que los datos personales se han cosificado. Nuestra información personal se ha cosificado y monetizado hasta tal punto que hemos perdido de vista que los datos personales, el objeto de nuestra privacidad, es el contenido de un derecho fundamental y que su fundamento último, y punto de partida, es la dignidad y desarrollo personal (Cotino Hueso, 2022b: 72, 76 y 98)[8].

Todos recordaremos artículos de prensa en los que se habla del valor de los datos, del valor del nuevo petróleo del siglo XXI, o de la nueva gasolina[9].

---

5 Reglamento (UE) 2016/679, del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta el tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE L 119, de 4 de mayo).

6 Art. 2 RGPD.

7 Así lo mantuvo ya el Tribunal Europeo de Derechos Humanos (TEDH) en su Sentencia de 16 de febrero de 2000, asunto Amann contra Suiza, § 65.

8 Sobre el problema de la cosificación del derecho fundamental a la protección de datos, y con ello, la cosificación de la persona, vid. la Recomendación sobre la ética de la Inteligencia Artificial, aprobada por la UNESCO en su 41ª Conferencia General, celebrada en París el 22 de noviembre de 2021 (41 C/73), donde se afirma que "las personas nunca deberían ser cosificadas, su dignidad no debería ser menoscabada de ninguna otra manera, y sus derechos humanos y libertades fundamentales nunca deberían ser objeto de violación o abusos", Apdos. 13-16 Anexo.

9 Por dar algunas cifras, un estudio de la UOC recoge que los datos de una persona tienen un valor en el mercado negro de Internet, en lo que se denomina Deep web o Internet profunda, de unos 870 euros. Vid. "Tus datos personales en Internet valen 870 euros", en Actualidad UOC, de 9 de enero de 2020 (Disponible en https://www.uoc.edu/portal/es/news/actualitat/2020/006-vender-datos-personales-internet.html#:~:text=Tus%20datos%20personales%20en%20internet%20valen%20870%E2%82%AC).

Pero este valor puede variar en función del tipo de información, siendo los datos de imágenes personales o *selfies*, así como los de historiales médicos, los más cotizados, alcanzando cifras de hasta 60 dólares. Por si esto no fuera suficiente, sólo hace falta recordar las desorbitadas cantidades que se han pagado por WhatsApp o por Twitter[10], lo que parece que no ha sido por su infraestructura tecnológica, sino por la información de sus usuarios y por su capacidad de control y de manipulación de los mismos.

Ninguna aplicación informática es gratuita. Detrás de esa generosidad de las multinacionales nos encontramos que la moneda de cambio somos nosotros y ejemplo de ello es la publicidad que aparece en aplicaciones como Instagram, Facebook o TikTok, publicidad personalizada en función de los intereses que conocen de nosotros, por la información que recopilan de los metadatos de nuestra navegación o simplemente porque nos escuchan, hace que se sustenten estos gigantes.

Hablamos, por tanto, de derechos fundamentales que hay que proteger, y en concreto del derecho a la protección de datos o de la privacidad en un sentido más amplio. Y aquí, debemos tomar como punto de partida la relación de la privacidad con la dignidad humana y el libre desarrollo de la personalidad, de la que son fundamento, así como el papel que juegan los datos personales y su control como conformadores de nuestra identidad (ahora digital) y de nuestro desarrollo personal.

No podemos por tanto perder de vista que lo que está en juego son derechos y esto es fundamental para focalizar nuestro objetivo y legislar en un sentido correcto donde lo que protejamos sea la privacidad y no otros intereses geopolíticos, sociales o económicos. Esto implica adoptar una visión "antropocéntrica" y "antropogénica", donde "la dignidad personal sea el impulso de las obligaciones jurídicas" (Cotino Hueso, 2022b: 71)[11].

10 Sobre estas cifras, vid. "¿Por cuánto se compraron las otras redes sociales", en Ara, de 26 de abril de 2022 (Disponible en https://es.ara.cat/economia/redes-sociales-precio-valor-compra-linkedin-twitter-whatsapp-instagram_1_4351369.html).

11 En este mismo sentido, vid. art. 7 Propuesta de Reglamento del Parlamento europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021) 206 final). Dicho art. lleva por título "Inteligencia artificial antropocéntrica y antropogénica".

Es fundamental analizar, en primer lugar, cómo se ve afectada la privacidad por este proceso de digitalización, especialmente por tecnologías disruptivas como la Inteligencia Artificial o el uso de algoritmos. En segundo lugar, se hace necesario analizar si este proceso de transformación digital nos permite hablar de derechos digitales y cómo encaja la privacidad en dicho nuevo contexto. Y aquí tendremos en cuenta, principalmente, no sólo el reconocimiento legal que hace nuestro ordenamiento jurídico de los derechos digitales en la LO 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante, LOPDGDD)[12], también los proclamados en la Carta de Derechos Digitales, presentada por nuestro Gobierno en julio de 2021[13]. Finalmente, debemos hacer una mención sobre el papel de los gigantes tecnológicos en este proceso de digitalización, algo que realmente preocupa en el funcionamiento de un Estado social y democrático de Derecho. Sólo de esta forma podremos concluir sobre cómo podemos afrontar estos nuevos desafíos digitales sin perder nuestra dignidad en el camino.

II. PRIVACIDAD Y TRANSFORMACIÓN DIGITAL

Es más que evidente –como en su día lo fue la Revolución industrial– que asistimos a un cambio de paradigma en nuestras sociedades, a un cambio cualitativo más allá de lo cuantitativo, a una nueva forma de ejercer los derechos y libertades por parte de los ciudadanos y a la forma de entender y aplicar el Derecho por parte de los Estados. Y todo ello marcado por la incertidumbre de lo que nos deparan el futuro y los avances tecnológicos, sus posibilidades y las amenazas para nuestros derechos (Fernández Rodríguez, 2020: 259-261; y Frosini, 1996: 88).

La mayoría de estas herramientas tecnológicas son altamente disruptivas porque están suponiendo un cambio radical y profundo en cualquier ámbito de nuestras vidas, dejando obsoletos mecanismos anteriores y representando un reto para nuestras sociedades. Toda esta realidad tecnológica nos está haciendo vivir un momento lleno de retos (Vázquez Alonso, 2022: 110; García

12 LO 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (BOE de 6 de diciembre).

13 Carta de Derechos Digitales española disponible en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

López, 2021). Asimismo, algo que tienen en común, por regla general, todas estas herramientas disruptivas o avances tecnológicos es el empleo de datos, de información personal.

La crisis que provocó el coronavirus hizo evidente la dependencia de las tecnologías digitales en todos los aspectos de nuestra vida, a la vez que mostró los peligros que las mismas traían de la mano. Tanto sector público como sector privado aceleraron su proceso de transformación digital y desencadenaron la aparición, el desarrollo y la evolución de todo un conjunto de tecnologías que trajeron ventajas, pero que también provocaron nuevas amenazas para los derechos y libertades de las personas.

Así pues, si bien el debate tecnología versus derechos fundamentales es una constante, durante la pandemia por coronavirus, se planteó con mayor intensidad un debate profundo sobre el uso de datos sobre nuestra salud, muchas veces sin guardar la proporcionalidad requerida en una medida que limitaba de derechos, aunque el fin perseguido fuera tan legítimo como protegen intereses vitales de la población. Nos referimos aquí, por ejemplo, al uso del llamado Pasaporte COVID o a la fallida puesta en marcha de la aplicación Radar COVID (Arenas Ramiro, 2020; y Arenas Ramiro, 2021)[14].

Esto es, se planteó el uso de la información personal de los ciudadanos, la limitación de su privacidad con un fin legítimo y aprovechando los avances y descubrimientos tecnológicos.

Por todo ello, teniendo en cuenta la actual capacidad de tratar y procesar datos personales y la más que probable pérdida de control personal sobre los mismos, entre los peligros para nuestra privacidad encontramos, como no podía ser de otra forma, la Inteligencia Artificial y el uso de algoritmos. La Inteligencia Artificial, incluida la elaboración de perfiles en la toma de

14 Noticias sobre esta cuestión, vid. "El fiasco de España con la "app" de rastreo del covid nos deja tres amargas lecciones", en *El Confidencial*, de 23 de junio de 2020 (Disponible en https://blogs.elconfidencial.com/tecnologia/homepage/2020-06-21/app-rastreo-contactos-covid-canarias-carme-artigas-sedia-sanidad-fernando-simon_2644739/); y "Radar COVID: cómo una app basada en el protocolo más respetuoso con la privacidad terminó sancionada por Protección de Datos", en *Newtral.es*, de 29 de junio de 2022 (Disponible en: https://www.newtral.es/radar-covid-sanciones-proteccion-datos-sancionada-aepd/20220629/), con referencia al procedimiento sancionador AEPD PS/00222/2021.

decisiones automatizadas, y el aprendizaje automatizado ponen en peligro nuestra privacidad. Asimismo, debemos destacar el hecho de que estas técnicas se usan de forma habitual y que con frecuencia ponen en peligro los derechos de los más vulnerables.

Estas nuevas tecnologías, que se han precipitado en los últimos años y especialmente durante la pandemia, se basan, sobre todo, como hemos dicho, en el uso masivo de datos personales, permitiendo una mayor recopilación, almacenamiento y análisis. Además, estos conjuntos de datos hacen que las personas sean vulnerables de varias maneras, ya sea a través de la exposición de sus datos, del intercambio con terceros, permitiéndose la identificación de la persona con los efectos que esto provoca en su identidad.

Incluso, aunque no se traten directamente datos personales, los avances tecnológicos, especialmente en este terreno, están impactando y modificando los derechos fundamentales, incluida la privacidad. Buscar información sobre patrones de comportamiento humanos y sacar conclusiones por técnicas probabilísticas y el uso de algoritmos, por ejemplo, para saber cuántas personas de una sala pueden profesar o no una determinada religión o el programa de televisión que prefieren, evidencia que hay que buscar nuevas garantías para el ejercicio de nuestros derechos en el entorno digital.

Esto no es solo una suposición o conjetura, sino una realidad puesta en práctica, por ejemplo, en China. En Xinjiang, provincia oeste de China, existen controles policiales, con reconocimiento facial, reconocimiento biométrico, videovigilancia y supervisión de las comunicaciones. Esto se añade al sistema de crédito social de China, que clasifica el comportamiento de sus ciudadanos y restringe el acceso al transporte y a buenos puestos de trabajo, entre otras cosas, a aquéllos que no cumplen los estándares. A finales de 2018 China denegó 5,5 millones de viajes en tren de alta velocidad y 17,5 millones de vuelos a viajeros que se encontraban en una lista negra y en julio de 2019 impidió que 2,56 millones de entidades desacreditadas adquirieran billetes de avión y que 90.000 compraran billetes de tren.

La cuestión es que muchas de las predicciones que los sistemas o algoritmos realizan afectan al libre desarrollo de la personalidad y que estas herramientas no están libres de errores porque siempre estarán rodeadas de la típica

incertidumbre que rodea a la probabilidad. Por ello, los resultados de sistemas de Inteligencia Artificial, que se basan en datos defectuosos o erróneos, pueden contribuir a las violaciones de derechos de muy distinta manera, introduciendo sesgos discriminatorios y pudiendo señalar a una persona como un probable terrorista o sospechoso de haber cometido un fraude. Esta situación la hemos visto también con los avances en las técnicas de reconocimiento facial o biométrico, incluyéndose información que revela características únicas de las personas con esos posibles efectos discriminatorios directos. De ahí la importancia, como luego veremos, de cumplir con los requisitos que la normativa establece para un correcto tratamiento de los datos personales, empleando datos de calidad, exactos y actuales.

Esta afectación de derechos fundamentales supone un atentado contra la esencia de la estructura de nuestros Estados. La limitación del poder de la información personal, del poder de disposición sobre nuestros datos personales tiene consecuencias no sólo para el propio titular del derecho, sino para la estructura democrática de nuestros Estados. Así, si una persona no controla o no sabe lo que se hace o se va a hacer con su información personal dejará de participar en la sociedad de la que forma parte, al margen de que nos encontraremos en una sociedad vigilada. Esto lo hemos visto, especialmente, en los sistemas que emplean los Estados con herramientas predictivas por el contexto de la prevención de delitos y de la seguridad nacional, o incluso en el desarrollo de los procesos electorales.

Esta cuestión, vinculada a la estructura de los Estados, en su óptica geopolítica, tiene auténtica relevancia, con dos actores principales que están marcando las líneas, por ejemplo, en la carrera del 5G y las ciudades inteligentes. La aparición de ciudades inteligentes basadas en 5G en Europa procede casi exclusivamente de China, a través de Huawei, su gigante de comunicaciones móviles. Estados Unidos está desarrollando 40 ciudades inteligentes, menos del 4 por ciento del total mundial, mientras que China está desarrollando 500, casi la mitad del total mundial, lo que ilustra la ventaja que saca Pekín al resto de países en esta carrera. Waterfront Toronto, un proyecto de ciudad inteligente de Sidewalk Labs, filial de Alphabet, ha sido objeto de críticas contundentes por el peligro que supone para la privacidad y la recopilación de datos que lleva a cabo. Roger McNamee, uno de los primeros inversores en Google y Facebook, afirmó que los datos obtenidos, sobre los usuarios en este

proyecto, tiene capacidad para sustituir la democracia con decisiones basadas en algoritmos y es una visión distópica que no tiene cabida en una sociedad democrática[15]. Para 2024, alrededor del 40 por ciento de la población mundial y unos 22.000 millones de dispositivos, desde coches hasta frigoríficos y desde teléfonos móviles hasta semáforos, estarán conectados a la red 5G, lo que cambiará por completo nuestro modo de vida.

El escándalo de *Cambridge Analytica* que sacudió a Facebook y los sesgos ideológicos de Google han generado un debate sobre la posible necesidad de romper con los gigantes tecnológicos por su transgresión en aspectos de privacidad, expresión y democracia.

En cualquier caso, ante los peligros a los que se enfrente la privacidad en este proceso de digitalización que vivimos, la idea no es prohibir el uso de la tecnología, sino que su uso se someta a un estricto control de legalidad y proporcionalidad con el fin de evitar actuaciones que, en aras de perseguir fines legítimos, bajo la opacidad de las mismas, impliquen el peligro de perpetuar discriminaciones y prejuicios sociales y raciales, por ejemplo.

De ahí que la privacidad se configure como uno de los pilares del Estado democrático. A mayor control personal del uso que se hace de sus datos personales, de su información personal, mayor participación ciudadana. Y este control personal de los datos personales en un entorno digital va a venir condicionado por la exigencia y cumplimiento de ciertos requisitos y principios recogidos, entre otras, en normas como las ya citadas, en el RGPD o en la LOPDGDD.

Sin detenernos en estos principios, pero dejándoles enunciados para que entendamos cómo se deben tratar los datos personales, como regla general, para que dicho tratamiento sea considera lícito y el sujeto pueda controlar sus datos personales, destacamos los llamados principios del tratamiento de datos (art. 5 RGPD), como el principio de lealtad, el principio de transparencia, el principio de minimización, la limitación de la finalidad, la limitación de la

15 Noticia sobre esta cuestión, vid. "La circulación masiva de datos pone en peligro la privacidad y las libertades individuales", en *EDJNet - The European Data Journalism Network*, de 13 de octubre de 2019 (Disponible en https://www.europeandatajournalism.eu/esl/Noticias/Noticias-de-datos/La-circulacion-masiva-de-datos-pone-en-peligro-la-privacidad-y-las-libertades-individuales).

conservación, el principio de seguridad o confidencialidad de la información y la responsabilidad proactiva. Y, de la misma forma, asimismo, necesitamos contar con una base de legitimación que permita tratar los datos personales (art. 6 RGPD), y aquí destacamos el hecho de que no todo se basa en el consentimiento de la persona.

Por todo ello, si se cumple con los principios del tratamiento de datos personales y se cuenta con una base de legitimación, partiremos de una premisa básica para tratar los datos personales y que los sujetos los controlen, garantizándose así un tratamiento de datos legítimo y protegiéndose su privacidad. La cuestión será comprobar si en este proceso de digitalización la privacidad necesita ser reconfigurada en el entorno digital, o si estamos ante un nuevo derecho digital, ante una nueva privacidad digital.

III. PRIVACIDAD Y DERECHOS DIGITALES. MÁS QUE NUEVOS DERECHOS, NUEVAS GARANTÍAS

En este proceso de transformación digital, los derechos deben replantearse y reconfigurarse –y, especialmente, garantizarse– en este nuevo escenario. La cuestión es analizar si se puede hablar o no de una privacidad digital y de si podemos o no entender que estamos ante un nuevo derecho digital. Por ello, lo primero es analizar lo que se entiende por derechos digitales y dónde se reconocen actualmente.

III.1. ¿Nuevos derechos?

Sin detenernos en normas y declaraciones de otros países[16], por lo que a España se refiere, no existen derechos digitales constitucionalmente reconocidos de forma expresa, pero nuestro Estado sí que ha querido reconocerles cierta entidad y desarrollarlos legalmente y así lo ha hecho en normas y declaraciones no vinculantes. Nos referimos, en primer lugar, a la LO 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD). Esta

16 Citamos aquí, por ejemplo, la *Declaración de Derechos en Internet (Dichiarazione dei Diritti in Internet)*, aprobada en Italia el 28 de julio de 2015; la Ley para una República digital (*Loi 2016-1321 pour une République numérique*), aprobada en Francia el 7 de octubre de 2016; o la Carta portuguesa de derechos humanos en la era digital (Carta Portuguesa de Direitos Humanos na Era Digital), aprobada por la Lei núm. 27/2021, de 17 de mayo de 2021.

norma, destinada a regular básicamente el tratamiento de datos personales, incluye en su Título X (artículos 79 a 97), de forma novedosa en nuestro ordenamiento jurídico, los llamados derechos digitales. Entre los derechos que la LOPDGDD reconoce en su Título X, se encuentran los derechos a la neutralidad de la Red así como el del acceso universal a Internet; los relacionados con la seguridad digital; los vinculados a los menores e Internet; los relacionados con los medios de comunicación digital; los relativos al ámbito laboral como el conocido derecho a la desconexión digital; o los vinculados con el tratamiento de la información personal y las facultades que otorga a sus titulares como el derecho al olvido en Internet o el testamento digital.

Todos estos "nuevos derechos" reconocidos como objeto de la LOPDGDD deberán ser garantizados conforme al mandato establecido en el art. 18.4 CE, esto es, limitando el uso de la informática[17]. No obstante, la mayoría de los derechos reconocidos requieren de un desarrollo legislativo o reglamentario posterior, lo que a finales de 2022 todavía no se ha producido.

En España, más allá de este reconocimiento formal a nivel legislativo, en segundo lugar debemos destacar la Carta de Derechos Digitales, aprobada por el Gobierno el 14 de julio de 2021, que aunque no tiene valor vinculante porque no es una norma jurídica, es todo un referente interpretativo a nivel nacional. Esta Carta reconoce, entre otros, los siguientes bloques de derechos: derechos de libertad como la identidad digital o el derecho al no perfilado; derecho de igualdad como el derecho de acceso y no discriminación; los derechos de participación y conformación del espacio público como la exigencia de información veraz; y los derechos del entorno laboral y empresarial.

No existe pues un derecho expresamente reconocido en nuestro ordenamiento jurídico como el derecho a una privacidad digital, o un derecho digital a la privacidad. La privacidad, como ha quedado dicho, tiene un carácter transversal a los citados derechos digitales, ya sea porque implican un tratamiento de datos personales, ya sea porque la privacidad, la facultad de control sobre la propia información personal, actúa como instituto de garantía de los mismos.

17 Art. 1.b) LOPDGDD.

No obstante, hay ciertos derechos de los llamados digitales que van a contribuir, unos más que otros, a garantizar la privacidad de los sujetos en el entorno digital. Nos referimos –más allá del derecho a la protección de datos personales garantizado como derecho digital en la Carta de Derechos Digitales de 2021[18], principalmente a tres derechos reconocidos en la Carta de Derechos Digitales de 2021, y a alguno más reconocido, en la LOPDGDD.

En primer lugar, hablamos del derecho a la identidad en el entorno digital[19]. Está claro que si garantizamos nuestra identidad en un entorno *online*, la imagen que de nosotros mismos hay en la Red, se protege nuestra privacidad.

Pero llegados a este punto debemos mencionar una cuestión relevante en relación con la privacidad y que excede el objeto de la misma y de su dimensión personal. Tenemos que hacer referencia aquí no sólo a una identidad personal individual, sino a una identidad digital colectiva. Las personas se desarrollan en sociedad y se reconocen no sólo de forma individual, sino por la pertenencia a un grupo y es, como grupo, donde tenemos un conjunto de datos que nos hacen valiosos y peligrosamente manipulables. Nuestra información personal cobra valor no tanto a nivel individual, sino por nuestra pertenencia a un grupo de sujetos con los mismos gustos, afinidades e ideologías. Por este motivo, en relación con este derecho, es donde cobra importancia controlar nuestra información personal y, por ello, hacer valer nuestro derecho al olvido[20].

En segundo lugar, nos referiremos al derecho al pseudonimato[21], aunque la Carta de Derechos Digitales no deja claro si lo que se garantiza es un derecho a tener un perfil con un pseudónimo, o bien, actuar en la Red de forma pseudonimizada. En todo caso, está claro que esta capacidad de ocultar nuestra identidad nos permite desarrollarnos de una forma más libre.

18 Art. III Carta de Derechos Digitales.

19 Art. II Carta de Derechos Digitales.

20 Art. 17 RGPD.

21 Art. IV Carta de Derechos Digitales.

Y, en tercer lugar, encontramos el derecho a no ser localizados ni perfilados[22]. Y aquí es necesario volver a referirnos a la colectividad, al grupo y debemos hablar de la llamada privacidad de grupo (Cotino, 2022b: 87-89; y Soriano Arnanz, 2021). Si bien las personas tenemos derechos a que no se nos perfile o catalogue, el verdadero y último peligro es que se manipule al grupo, que reúne una u otra cualidad. Es la misma idea de una identidad digital colectiva.

Hoy en día se pueden inferir sensibilidades, gustos o preferencias o futuras enfermedades por la vinculación con un determinado perfil. Es necesario conseguir y garantizar que los sujetos no se vean vinculados a un perfil. Y aquí es donde debemos acudir al RGPD, que en su art. 22, establece, con carácter general, la prohibición de los perfilados. El RGPD garantiza el derecho a no ser objeto de una decisión basada "únicamente" en un tratamiento automatizado, incluida la elaboración de perfiles. La cuestión en este punto será que las decisiones no sean "únicamente" automatizadas.

En este punto no hay que olvidar que este derecho se garantiza en tanto en cuanto estamos hablando de datos personales y que la cuestión se produce porque muchos de los datos empleados por las herramientas de Inteligencia Artificial o por los algoritmos que crean perfiles no son datos personales que identifiquen a una persona de manera individualizada, sino que lo hacen por su vinculación con un colectivo. Esto es, me pueden clasificar, y potencialmente manipular, no por mis convicciones o por mis características personales, sociales o económicas, sino por mi inclusión en un grupo con unas determinadas convicciones o características personales, sociales o económicas.

Este último extremo es lo realmente preocupante y peligroso para nuestros derechos fundamentales. Lo peligroso no es manipular o discriminar a una persona de manera individualizada (sin infravalorar el atentado a los derechos fundamentales de la misma), sino que se manipule a un colectivo. Así lo hemos visto en numerosos asuntos, destacando el conocido caso del escándalo de *Cambridge Analytica* en las elecciones presidenciales de Estados Unidos de 2016 que dieron la victoria a Donald Trump. Aunque también podemos destacar aquí que otro gran peligro es que, a raíz de un perfilado, se perpetúen

22 Art. V Carta de Derechos Digitales.

discriminaciones de colectivos más vulnerables porque nuestros algoritmos no cumplen con un mínimo de valores éticos en su configuración.

Junto a estos tres derechos, la Carta de Derechos Digitales hace referencia a los derechos digitales en entornos específicos, entre los que cita los derechos ante la Inteligencia Artificial y los derechos digitales en el empleo de las neurotecnologías[23]. La Carta indica que herramientas como la Inteligencia artificial deben asegurar un enfoque centrado en la persona y en su inalienable dignidad, destacando la importancia de cumplir con principios como la transparencia y la auditabilidad o rendición de cuentas, más allá de la accesibilidad universal. Y, al mismo tiempo, en relación con el empleo de neurotecnologías hace hincapié en la garantía de la autodeterminación individual y de la propia identidad. Todo ello refuerza la protección de la privacidad en el entorno digital y el control de nuestra información personal en el mismo.

III.2. Nuevas garantías

Si bien la LOPDGDD garantiza legalmente este conjunto de derechos a los que denomina digitales, no han faltado las voces que han evidenciado que si bien dicho reconocimiento es "loable", la propia norma rebaja estas expectativas de protección, al no otorgar a la mayoría de los artículos que reconocen estos derechos digitales el rango de ley orgánica y, por lo tanto, la máxima protección que nuestro ordenamiento jurídico garantiza a los derechos fundamentales[24]. Se evidencia así que, a pesar de que pueda existir una demanda social, existen dificultades de "materialización jurídica" (Rebollo Delgado / Zapatero Martín, 2019: 13-14).

Como han planteado reputados autores, las dudas no son sólo sobre su fundamento constitucional y sus mecanismos de garantía (al no ser reconocidos como derechos fundamentales)[25], sino que se plantean dudas sobre la nece-

23 Arts. XXV y XXVI Carta de Derechos Digitales, respectivamente.

24 Así se deduce de la Disposición Final Primera LOPDGDD, que señala que "La presente ley tiene el carácter de ley orgánica. No obstante, tienen carácter de ley ordinaria: (…) los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X".

25 Exigiéndose no sólo su regulación por Ley orgánica como se deriva del art. 81 CE, sino el resto de las garantías normativas y jurisdiccionales.

saria actuación por parte de los poderes públicos no sólo para garantizar un acceso universal a la Red, sino para garantizar el pleno desarrollo personal en el entorno digital (Rallo Lombarte, 2021: 101 y 104).

No obstante, aunque es la propia LOPDGDD la que indica en su art. 79, como ha quedado dicho, que los derechos digitales que recoge son los tradicionales derechos adaptados a la Era digital[26], la misma norma indica en su Preámbulo que los derechos digitales que reconoce en su Título X deberían incluirse en la deseable reforma de nuestro texto constitucional, ya que esta reforma, según reza la LOPDGDD "debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales"[27].

Si bien esto puede parecer contradictorio, entendemos que más que reconocer nuevos derechos digitales, la esencia debería ser dotar a los derechos tradicionalmente reconocidos en nuestro texto constitucional de una mayor protección y seguridad jurídica adaptándolos al imparable proceso de digitalización y de Internet. Como en su día señaló Rodotà, "las nuevas realidades producidas por la ciencia y la tecnología hacen que la sociedad pida al derecho seguridad, más que protección" (Piñar Mañas, 2018: 105; Rodotá, 2010: 12). Si las nuevas demandas sociales no tuvieran su reflejo en los derechos ya reconocidos constitucionalmente, sólo entonces podríamos hablar de la necesidad de reconocer nuevos derechos (Cotino Hueso, 2022b: 72; y Escobar Roca, 2018: 99 y ss.).

El proceso sería pues digitalizar nuestro texto constitucional y reorientar los mecanismos de protección de nuestros derechos fundamentales teniendo en cuenta el nuevo entorno digital y sus amenazas (Cotino Hueso, 2022b: 70; y Balaguer Callejón, 2021).

26 Señala la LOPDGDD "Artículo 79. Los derechos en la Era digital. Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación".

27 Preámbulo LOPDGDD.

Así las cosas, a falta de reconocimiento constitucional, las nuevas garantías deberían venir de reforzar los principios tradicionalmente reconocidos en las normas vigentes en materia de protección de datos personales, al mismo tiempo que se reconocían principios éticos, una perspectiva ética, pero jurídicamente exigibles.

El uso de los datos personales y de herramientas como la Inteligencia artificial debe realizarse garantizando la igualdad, la rendición de cuentas y la transparencia. El enfoque del uso de la información personal debe ser un enfoque basado en la protección y garantía de los derechos humanos. De esta forma, se potenciarán los beneficios del progreso tecnológico y se minimizarán los daños y peligros que éstos representan.

Como ha quedado dicho, se debe situar en el centro de la protección a la persona. En esta línea, más allá de la LOPDGDD y la citada Carta de Derechos Digitales, a nivel europeo, aunque sin carácter vinculante encontramos en primer lugar la *Declaración sobre los Derechos y Principios Digitales para la Década Digital*[28], aprobada en Europa el 26 de enero de 2022 y estableciendo la necesidad de dar prioridad a las personas, situar a la persona en el centro de la transformación digital, debiendo la tecnología proteger los derechos de las personas, esto es, estar al servicio y beneficio de todos los ciudadanos europeos. En segundo lugar, y con carácter vinculante –cuando se apruebe definitivamente–, encontramos la Propuesta de Reglamento sobre Inteligencia Artificial, presentada el 21 de abril de 2021[29].

Para que exista un respeto a nuestra privacidad y a nuestros derechos digitales es necesario que los avances tecnológicos y, muy especialmente, herramientas como la Inteligencia Artificial y los algoritmos, cumplan con una serie de principios como el de no discriminación, rendición de cuentas y transparencia.

28 Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, Bruselas, 26 de enero de 2022 (COM (2022) 28 final).

29 Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021) 206 final). Asimismo, vid., posteriormente, la Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la Inteligencia Artificial en la era digital (2020/2266(INI)).

Todos ellos principios ya reconocidos, entre otras normas, en el citado RGPD así como en la propuesta de Reglamento de Inteligencia Artificial.

Pero, además, es esencial que, como toda injerencia en un derecho fundamental, ésta cumpla con los requisitos que se exigen a los mismos para ser legítimos. A saber, en primer lugar, la necesaria previsión legal se requiere de una norma clara y previsible. Y esto es uno de los principales problemas de nuestro ordenamiento jurídico. En segundo lugar, se requiere una finalidad legítima, lo que se da por hecho. En tercer lugar, se debe superar el test de proporcionalidad, esto es, su necesidad en una sociedad democrática. Y da igual que la afectación del derecho a la privacidad o a cualquier otro derecho digital se produzca en un entorno digital o no. Por ello, se hace necesario evaluar el impacto de la privacidad de los sujetos de las medidas que pueden limitar sus derechos. Las evaluaciones de impacto, reguladas en el RGPD[30], son el mecanismo idóneo y esencial para verificar si la medida a implementar, si la herramienta a diseñar, supondrá o no un impacto negativo en nuestra privacidad.

Y damos un paso más allá. No sólo se requieren normas claras y precisas y un estricto cumplimiento del test de proporcionalidad, sino que se requiere una evaluación del impacto en la privacidad de los sujetos atendiendo a valores éticos y no discriminatorios. En esta línea se dirigen los esfuerzos europeos y no solo con la propuesta de Reglamento sobre Inteligencia Artificial, sino con las conocidas "Directrices éticas para una IA fiable" (*Ethics guidelines for trustworthy AI*), del Grupo de Expertos de Alto nivel de la UE para IA, publicadas ya en abril de 2019[31], y que se centran en tres componentes: que la Inteligencia Artificial sea licita, que sea ética y que sea robusta desde el punto de vista técnico y social. Estas orientaciones pivotan alrededor de la transparencia con las exigencias de facilitar la trazabilidad y la auditabilidad de los

30 Art. 35 RGPD.

31 Las Directrices éticas para una IA fiable (*Ethics guidelines for trustworthy AI*), aprobadas por el Grupo independiente de Expertos de alto nivel sobre Inteligencia artificial creado por la Comisión Europea en junio de 2018, publicadas el 8 de abril de 2019. Disponibles en: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

sistemas de Inteligencia Artificial, o la promoción y formación y la educación con el fin de conocer una Inteligencia Artificial fiable[32].

Pero esta labor no se puede dejar sólo en manos de los Tribunales. Debemos dotar de mayores facultades de control y de sanción a las Autoridades de control de protección de datos para que nos ayuden en este proceso complejo. Debemos detenernos para reflexionar sobre la forma en la que queremos configurar los derechos y valores de nuestra sociedad. Y lo debemos hacer ahora, porque lo que definamos ahora será lo que marcará las sociedades del futuro. Debemos pensar en cómo construir una sociedad digital más justa e igualitaria, evitando replicar los problemas, los estereotipos y los comportamientos discriminatorios que existen en los entornos no digitales y esto sólo se pude hacer con transparencia y rendición de cuentas.

Por ello, la persona debe estar en el centro de una nueva ética digital, los datos deben estar al servicio de la humanidad, con un mayor respeto por la dignidad humana[33]. De ahí la necesidad de su configuración conforme a Derecho y siguiendo unos principios y valores éticos (Rodotá, 2018: 87-94). Esto debe ser no sólo auditable, sino exigible.

IV. LOS GIGANTES TECNOLÓGICOS, LA AFECTACIÓN A LA PRIVACIDAD Y SU PAPEL EN LA TRANSFORMACIÓN DIGITAL

El potencial disruptivo de estas grandes empresas es más que evidente. El crecimiento de las plataformas de redes sociales tiene profundas implicaciones en la forma en la que trabajamos, en cómo aprendemos, cómo nos relacionamos en sociedad y cómo participamos en la misma. De hecho, la Red ha cambiado la forma en la que entendemos el mundo y la forma en la que nos desarrollamos y configuramos nuestra personalidad, ahora digital (Moret

32 En las Directrices éticas para una IA fiable se recogen y desarrollas siete principios para alcanzar una Inteligencia Artificial fiable, a saber: intervención y supervisión humanas; robustez y seguridad; privacidad y gestión de datos; transparencia; diversidad, no discriminación y equidad; bienestar social y medioambiental; y rendición de cuentas.

33 Así lo indicó el SEPD en su Dictamen 4/2015 sobre ética digital.

Millás / Sánchez Gil, 2022: 289), así como la forma en la que somos ciudadanos. Y esto afecta y configura, entre otros derechos, nuestra privacidad.

La digitalización no se trata de una cuestión que afecte exclusivamente al sector público. La propia naturaleza de la transformación digital ha convertido a los operadores privados en un agente de primer orden en la garantía, o posible lesión, de los derechos fundamentales, con independencia de su tamaño o localización. Se ha mantenido que esto ha provocado que los titulares de derechos sean vistos como consumidores ante la cosificación de sus derechos (Cotino Hueso, 2022b: 76-77; Balaguer Callejón, 2019; y Sánchez Barrilao, 2016: 256).

Más aún, estas grandes compañías no sólo afectan a los derechos en el entorno digital derechos que ellas no ejercen, y que alegan para ser vistas como meras intermediarias (Villaverde Menéndez, 2007: 38), sino que, más allá de interferir en la propia estructura de nuestros Estados, interfieren en el funcionamiento del mercado, dado que las grandes tecnológicas, que poseen el suficiente *knowhow* y la experiencia o experticia, tendrán una ventaja competitiva y un poder jamás visto (Ausin / Morte / Monasterio, 2020).

Estas grandes tecnológicas han forjado monopolios transnacionales con una capacidad y un poder jamás visto capaz de analizar el comportamiento humano y predecirlo, con la posibilidad de influir en el mismo y en la formación de la opinión pública y, por lo tanto, en la estructura de nuestros Estados, rompiéndose así la idea de que Internet y estas propias compañías iban a contribuir a crear un foro de discusión abierto y alejado de la concentración y supuesta manipulación que venían ofreciendo los medios de comunicación tradicionales (Vázquez Alonso, 2022: 114; y Khan, 2017).

Los Estados, pese a estar encargados de controlar la actividad de los gigantes tecnológicos situados en su territorio, no cumplen con su deber a causa de su importancia para la economía nacional. Entre enero de 2010 y junio de 2020, Amazon, Facebook, Google y Apple han realizado en Irlanda un total de 14 inversiones destinadas a proyectos de las TIC y de infraestructura, cuyo importe económico asciende a 7130 millones de euros desde 2010. Microsoft anunció una inversión de 1500 millones de dólares en Italia para la computación en la nube. Siguiendo esta misma línea, también realizará una inversión

de mil millones de dólares en Polonia. Google confirmó que invertiría entre 1500 y 2000 millones de dólares en un CPD en Polonia para administrar los servicios en la nube. La integración de las grandes compañías tecnológicas en los países europeos es total. Por ejemplo, el diplomático danés Casper Klynge ocupa actualmente la vicepresidencia de Microsoft para asuntos gubernamentales europeos en Bruselas.

Conforme la sociedad se va digitalizando el nivel de dependencia en los gigantes tecnológicos se incrementa. El papel de la UE como entidad, así como la de sus Estados miembros es evitar justamente que estas entidades tengan un poder supranacional evitando además que no se convierta en una guerra geopolítica, pero la clara influencia económica y política de estas corporaciones hace que sus propias fronteras como empresas privadas se difuminen.

A pesar de lo dicho los grandes gigantes tecnológicos comienzan a experimentar un creciente desgaste en su reputación –por ejemplo, con la gestión de nuestros datos, *big data* y uso de redes sociales para intentar influir de manera ilícita en unas elecciones, como ha quedado dicho–. La visión positiva de estas empresas tecnológicas como ejemplo de innovación y actores en el nuevo mundo comienza a desgastarse al percibirse más un poder incontrolable con consecuencias profundas y perversas en la política y la industria.

Al final, son estos gigantes tecnológicos los que están configurando nuestros derechos fundamentales, los que están adoptando una posición que tendrían que ocupar los poderes del Estado o, al menos, estar controlados por éstos. Es cierto que se requiere su colaboración, pero de la mano de unas políticas públicas claras y efectivas que limiten las actividades comerciales de estas empresas tecnológicas y, dando un paso más allá, colaboren con ellas para corregir las disfuncionalidades existentes (Rallo Lombarte, 2021: 112; y García Mexía, 2017).

La cuestión es si son ellos los que pueden ofrecer las garantías adicionales adecuadas para el ejercicio de los derechos en un entorno digital del que son los dueños, o si, por el contrario, los sitúan ante un peligro mayor. Según *Transparency International*, entre 2009 y 2018, Google contrató a un total de 23 funcionarios de instituciones europeas, 11 de los cuales ejercen presión

específicamente en la UE, lo que pone en evidencia el fenómeno de las puertas giratorias en dichas instituciones.

Estas grandes tecnológicas están configurando nuestros derechos, de una u otra forma. Si ya hemos citado los casos de manipulación electoral o de desinformación, un claro ejemplo de la intervención de estos gigantes tecnológicos en nuestros derechos ejercidos en Internet, especialmente de nuestra vida privada, lo encontramos, por ejemplo, en un caso de 2014 ante el Tribunal de Justicia de la Unión Europea (TJUE) donde se analizó la existencia del llamado derecho al olvido (el conocido caso Costeja contra Google)[34]. El fallo del TJUE tras la demanda de un ciudadano español que solicitaba a Google ser borrado de las búsquedas de su buscador, a pesar de que la información en origen había sido publicada lícitamente, obligaba a Google a ejecutar el derecho al olvido solicitado, pero tras la correspondiente valoración y ponderación con otros derechos e intereses en juego.

Vemos cómo son los buscadores de Internet, como Google, los que, en último término ponderan y deciden si una información debe ser o no suprimida de Internet y, por lo tanto, deciden en último lugar a qué información accederemos o no los ciudadanos cuando hagamos uso de sus servicios. Es más que evidente que se produce una afectación que procede de los prestadores de servicios de Internet quienes, como empresas privadas, "no están en condiciones de ponderar derechos y bienes jurídicos adecuadamente, porque se rigen por las reglas de mercado" (Pauner Chulvi, 2018: 300, 304-305 y 310).

Por ello, debemos entender que el sector privado es protagonista y tiene no solo responsabilidad, sino una gran influencia, no tanto por los contenidos porque no son editores en sentido estricto, pero sí porque interfieren en el ejercicio de los derechos.

Esto exige contar con un sector privado que opere como un protagonista comprometido y proactivo a la hora de investigar, innovar y emprender, y que lo haga desde la ética de la garantía de los derechos fundamentales. Pero también implica exigir responsabilidades, por su responsabilidad cívica o ética y democrática, y limitar su actuación frente a posibles riesgos generados por

34 STJUE de 13 de mayo de 2014, caso Google contra AEPD / Mario Costeja (C-131/12).

su actuación porque es a través de su tecnología y de las herramientas que generan cómo condicionan el ejercicio de nuestros derechos, requiriéndose, por lo tanto, la intervención política de los Estados y no dejándose nuestros derechos y la estructura de nuestros Estados, en manos de la buena voluntad de estos gigantes digitales (Vázquez Alonso, 2022: 121-122).

Así las cosas, aunque inicialmente estas empresas, que ofrecen una gran variedad de servicios en el mercado digital, fueron vistas como meros intermediarios en la gestión de los contenidos caracterizados por su "neutralidad"[35], esta visión está cambiando, especialmente en Europa[36]. Ese deseo liberal de no injerencia estatal provocó la aprobación de normas que eximían de responsabilidad a los proveedores de servicios de Internet por los contenidos que publicaban o compartían[37], apelándose a la llamada doctrina jurídica del "buen samaritano",

35 Una neutralidad que se exigía de la Red con el fin de crear un foro de discusión libre y sin deseos, ni atisbos, de querer ser regulado. Sobre la neutralidad de la red, véase el pronunciamiento del TJUE sobre este Reglamento 2015/2120 (Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) nº 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión (DOUE núm. 310, de 26 de noviembre de 2015), que consagra el principio esencial de apertura de Internet o neutralidad de la Red (art. 3). El TJUE condenó a una compañía por ralentizar o bloquear servicios que quedaban al margen de la llamada facturación cero (lo que también se conoce como *zero rating*"). Vid. STJUE de 15 de septiembre de 2020, asunto Telenor Magyarország (C-807/18).

36 Vid. *Loi núm. 2020-766, du 24 juin 2020, visant à lutter contre les contenus haineux sur Internet* (Ley núm. 2020-766, de 24 de junio de 2020, destinada a combatir el contenido de odio en Internet) (JORF núm. 0156, de 25 de junio de 2020. Disponible en https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970); y Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) vom 1. September 2017 (Netzwerkdurchsetzungsgesetz - NetzDG) (Ley, de 1 de septiembre de 2017, para la mejora de la aplicación de la ley en las redes sociales) (BGBL I S. 3352. Disponible en https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html).

37 Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DOCE, núm. 178, de 17 de julio de 2000). Vid., arts. 14 y 15 Directiva sobre el comercio electrónico. Y, por todos, el Título V en la Ley de Telecomunicaciones de 1996. Vid. 47 U.S. Code § 230 - *Protection for private blocking and screening of offensive material*. Señala la Sección 230 de la *Communications Decency Act* que: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".

bajo la presunción de que las Plataformas de redes son intermediarios pasivos que actúan simplemente como "plazas públicas" a través de las cuales los usuarios se comunican entre sí (Vázquez Alonso, 2022: 111; Keats / Wittes, 2017; y Wu, 2003). Todo lo que se comprueba que no es cierto y de ahí la exigencia de responsabilidad (Moret Millás y Sánchez Gil, 2022: 292).

Por todo ello, como ya adelantamos, estos gigantes tecnológicos no pueden ser considerados como empresas neutrales. Asistimos aquí a un progresivo "levantamiento del velo" respecto a la verdadera naturaleza jurídica de estas empresas, pues como se ha dicho, son más que meros intermediarios a la hora no sólo de tratar la información, sino de compartirla (Vázquez Alonso, 2022: 115).

Ello obliga, también, a innovar el ordenamiento jurídico tanto desde el punto de vista del entendimiento tradicional de los derechos como límites al poder público, como desde la óptica de las garantías. Los derechos no son sólo límites al poder público. No podemos hablar sólo de las obligaciones positivas de los poderes públicos para garantizar nuestros derechos, sino que ante las amenazas del sector privado, especialmente en este terreno de estas grandes compañías, que lo saben todo de nosotros, debemos acabar hablando de una eficacia horizontal (*Drittwirkung*) entre particulares. Por poner un ejemplo, la manipulación electoral en las redes, los debates extremos que incitan al odio polarizando a la sociedad, o la desinformación dependen de la existencia de plataformas tecnológicas que se lucran con tales actividades.

Se hacen necesarias normas que regulen esta transformación digital y de que los Estados asuman que una regulación es necesaria porque todo mercado necesita de una regulación, no teniendo sentido la eterna dicotomía entre Estado y mercado. No puede dejarse la cuestión totalmente a lo que ellas decidan ni en clave estratégica e internacional, ni respecto del ámbito electoral, ni en general. Sus intereses privados en modo alguno tienen por qué alinearse con los intereses nacionales ni con los intereses públicos y derechos fundamentales de la ciudadanía en juego. De ahí que es necesario ver qué fórmulas de regulación emplear para hacer prevalecer tales intereses y derechos en juego.

La cuestión está en determinar el grado de implicación y responsabilidad que quiera atribuírselas, o que los Estados puedan y quieran atribuirlas.

En este punto se ha planteado que, dada su posición, su estatuto jurídico debería ser como el de los entes específicamente vinculados a la consecución del interés general o, como se ha mantenido acertadamente, como de "entes vicariales del Estado", en tanto ejercen las funciones que deberían ser competencia del Estado, y, en ocasiones, actúan por cuenta de éste, llegando donde el Estado no puede (o no quiere) llegar, como vimos que pasó en el caso Google, donde el TJUE condenó a Google a actuar ponderando derechos, competencia exclusiva de los órganos jurisdicciones o de los Tribunales o Cortes Constitucionales. En el entorno digital, estos gigantes tecnológicos están ejerciendo un poder que no es estrictamente privado, pasando a ocupar un espacio público (Balaguer Callejón, 2022). De ahí que, dado el "progresivo ensanchamiento de su responsabilidad", se deba limitar la autonomía que para decidir y fiscalizar su propia actuación se les reconoce a estos gigantes tecnológicos (Vázquez Alonso, 2022: 115 y 118; y Rodríguez-Izquierdo, 2019: 77-100).

Así pues, con el fin de regular la actuación de los gigantes tecnológicos en el proceso de digitalización de nuestras sociedades y de nuestros derechos, con el fin de hacer responder a estos gigantes tecnológicos por sus responsabilidades cívicas, éticas o democráticas, como ha quedado dicho, pero sobre todo en relación con el control de los contenidos de los que son responsables, se aprobó en julio de 2022 y se publicó en octubre de 2022, un Reglamento conocido como la Ley de Servicios Digitales (*Digital Services Act*, DSA)[38], que

38 Reglamento (UE) 2022/2065, de 19 de octubre de 2022, del Parlamento europeo y del Consejo, relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales) y por el que se modifica la Directiva 2000/31/CE (DOUE L 277, de 27 de octubre de 2022) (en adelante, DSA). La propuesta fue aprobada el 5 de julio de 2022 y entrará en vigor a los veinte días de su publicación el 27 de octubre de 2022 en el DOUE. Junto a la DSA se aprobó otra norma, otro Reglamento conocido como la Ley de Mercados Digitales (*Digital Markets Act, DMA*), definiendo bajo criterios estrictamente objetivos las condiciones para que una gran Plataforma en línea pueda ser considerada como "guardián de acceso" (gatekeeper) y, en base a ello, fijar una serie de obligaciones que velen por un entorno empresarial que garantice "una mayor oferta de servicios para los consumidores". Este último Reglamento (la DMA) se publicó en el DOUE L 265, de 12 de octubre (finalmente, Reglamento (UE) 2022/1925, del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

será aplicable, con carácter general, a partir del 17 de febrero de 2024[39]. Se les hace así responsables de los contenidos ilícitos que alojen o arrojen con sus servicios, ya que hasta ahora, como hemos visto, no lo eran si demostraban no tener conocimiento efectivo de la situación ilícita, como recoge la ya citada Directiva sobre el Comercio electrónico del año 2000. Las soluciones que se están presentando en la Unión Europea ponen su acento en el compromiso y la colaboración de estos grandes operadores, apostándose tanto por la regulación como por la colaboración.

El propio Reglamento reconoce que los "servicios de la sociedad de la información y especialmente los servicios intermediarios se han convertido en una parte importante de la economía de la Unión y de la vida cotidiana de sus ciudadanos", a la vez que se reconoce que "la transformación digital y el creciente uso de esos servicios también entraña nuevos riesgos y desafíos para los destinatarios de los servicios a título individual, las empresas y la sociedad en su conjunto"[40]. Y, por ello, se establecen obligaciones para los proveedores de servicios digitales de forma proporcional al tamaño de las Plataformas digitales y en función de los riesgos que representan para la ciudadanía, siendo las de "muy gran tamaño" las que tengan un número de usuario mayor al 10% de la población de la Unión Europea, esto es, unos 45 millones de usuarios (Moret Millás / Sánchez Gil, 2022: 311-312)[41].

La nueva norma obligará a las grandes empresas tecnológicas a evaluar y gestionar los riesgos sistémicos, como la apología del odio y la difusión de desinformación que presentan sus servicios, y se les exigirá someterse a auditorías anuales independientes, y proporcionar a los organismos reguladores el acceso a los datos de las plataformas e información sobre las llamadas "cajas negras" de sus algoritmos para garantizar un mayor nivel de transparencia

39 Art. 93.2 DSA, que indica que a pesar de la citada fecha: "No obstante, el artículo 24, apartados 2, 3 y 6, el artículo 33, apartados 3 a 6, el artículo 37, apartado 7, el artículo 40, apartado 13, el artículo 43 y las secciones 4, 5 y 6 del capítulo IV, serán de aplicación a partir del 16 de noviembre de 2022".

40 Considerando 1 DSA.

41 Art. 33 DSA.

y rendición de cuentas[42]. Asimismo, establece un régimen sancionador con multas económicas de hasta el 6 % del volumen de negocios mundial anual[43]. Pero la DSA destaca, especialmente, y para lo que aquí nos interesa, por establecer un modelo de co-regulación, donde no sólo estarán implicados las grandes tecnológicas, sino que el Estado deberá velar por los intereses públicos en juego, limitándose así la opacidad y total discrecionalidad de estos gigantes (Cotino Hueso, 2022a: 217-219 y 236-237)[44].

En esta línea, el Reglamento de Servicios Digitales se refiere a una corregulación, aunque no creemos que la configuración de un derecho fundamental se pueda dejar en manos del sector privado. Asimismo, a esto debemos añadir que entendemos que el sector público debería ser sometido a un régimen sancionador desde la óptica del *compliance*, más allá del mero apercibimiento recogido en la LOPDGDD (art. 77.2 RGPD). De esta forma se incentivaría el cumplimiento por el sector público, que en la actualidad ante una infracción no ven una repercusión económica ni la pérdida reputacional que tendrá dicha repercusión.

Por último, junto a las previsiones de la DSA, norma pionera a la hora de exigir responsabilidades a las grandes Plataformas y de imponerles un conjunto de obligaciones, el Supervisor Europeo de Protección de Datos (SEPD) nos ha recordado la necesidad de mecanismos de control no sólo internos, sino externos, "sistemas de control que aseguren el cumplimiento y proporcionen evidencia relevante, en particular, a las Autoridades de supervisión independientes"[45].

---

42 Destacamos, Considerando 79 y art. 34 DSA sobre evaluación del riesgo o el art. 37 DSA sobre las auditorías independientes.

43 Art. 52 DSA.

44 Vid. Considerando 104 DSA.

45 Opinión 4/2015 del SEPD "*Towards a new digital ethics. Data, dignity and technology*", de 11 de septiembre de 2015. Ya en 2020, cuando se adoptó la Propuesta, el 15 de diciembre, por el Parlamento Europeo y por el Consejo, el SEPD se pronunció en la *Opinión 1/2021 sobre la Propuesta de Ley de Servicios Digitales*, adoptada el 10 de febrero de 2021, manifestado su apoyo a un entorno en línea transparente y seguro, definiendo responsabilidades y rendición de cuentas.

Sin embargo, el Paquete de Servicios Digitales sólo puede ser eficaz si las grandes empresas tecnológicas cumplen las normas en la práctica. La Comisión Europea y los reguladores nacionales deben ahora poner el foco en la supervisión y el cumplimiento. Hacer que las plataformas cumplan las normas requerirá suficientes recursos humanos y técnicos, incluidas las herramientas y los conocimientos informáticos necesarios.

V. BREVE REFLEXIÓN FINAL

Nuestra privacidad, el control y poder de disposición de nuestra información personal, cuya esencia es la dignidad persona, debe reinterpretarse en el entorno digital donde herramientas como la Inteligencia Artificial y los algoritmos son, –más allá de los beneficios que éstas aportan–, sus principales amenazas.

La falta de un reconocimiento constitucional a las garantías de nuestros derechos en los entornos digitales provoca que sean los gigantes tecnológicos los que estén interfiriendo no sólo en su configuración, sino en la medida de sus garantías.

Por ello, la convivencia con los gigantes tecnológicos debe estar presidida por el objetivo de la protección, y desarrollo, de los derechos, que tienen que adecuarse, rápida y eficazmente, a la velocidad con que crecen y se desarrollan los avances tecnológicos como la Inteligencia Artificial y los algoritmos, entre otros.

Junto con ello, la formación y desarrollo de competencias digitales de los actores implicados, y fundamentalmente de los usuarios, es prioritario en esta convivencia porque el afectado es el principal garante de sus derechos y el que más oposición y limitación puede hacer a los principales operadores de Internet y de redes sociales. La formación en competencias digitales reconocida por nuestra LOPDGDD supone la base normativa para justificar la exigencia de la capacitación de la sociedad en competencias digitales.

Asimismo, y en último lugar, debemos indicar que la aprobación de normas en este entorno, o el reconocimiento constitucional del entorno digital, no será suficiente si las mismas no van "impregnadas" de valores éticos, pero exigibles jurídicamente. Sólo de esta forma podremos situar a la persona

en el centro de la protección de la transformación digital. Como indica la Carta de Derechos Digitales española, "la persona y su dignidad son la fuente permanente y única de los mismos y la clave de bóveda tanto para proyectar el Ordenamiento vigente sobre la realidad tecnológica, como para que los poderes públicos definan normas y políticas públicas ordenadas a su garantía y promoción"[46]. De nuevo, la tecnología al servicio de la humanidad.

VI. BIBLIOGRAFÍA

– ARENAS RAMIRO, M. (2020): "¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos", en: *Revista La Ley Privacidad*, núm. 5, p. 49.

  - (2021): "Pasaporte COVID, ¿libertad de circulación de forma segura o discriminación y privacidad en juego?", en: *Revista La Ley Privacidad*, núm. 8, p. 20.

– AUSIN, T. / MORTE, R. / MONASTERIO, A. (2020): "Neuroderechos: derechos humanos para las neurotecnologías", en: *Diario La Ley*, núm. 43, Sección Ciberderecho, de 8 de octubre de 2020.

– BALAGUER CALLEJÓN, F. (2019): "Redes sociales, compañías tecnológicas y democracia", en: *Revista de Derecho Constitucional Europeo*, n.º 32, julio-diciembre.

  - (2021): "La Constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital", en: GOMES, A. C. y otros (Coords.), *Direito Constitucional: diálogos em homenagem ao 80º aniversário de J. J. Gomes Canotilho*. Belo Horizonte: Fórum, Brasil.

  - (2022): "O impacto dos novos mediadores da era digital na liberdade de expressão", en: *Espaço Juridico: Journal of Law*, Vol. 23, nº 1, pp. 179-204.

46 Consideraciones previas Carta Derechos Digitales.

– COTINO HUESO, L. (2022a): "Quién, cómo y qué regular (o no regular) frente a la desinformación", en: *Teoría y Realidad Constitucional*, núm. 49, pp. 199-238.

- (2022b): "Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", en: *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor, España, pp. 69-105.

– ESCOBAR ROCA, G. (2018): *Nuevos derechos y garantías de los derechos*, Marcial Pons, Madrid.

– FERNÁNDEZ RODRÍGUEZ, J. J. (2020): "Derechos y progreso tecnológico: pasado, presente y futuro", en: ENGELMAN, W., *Sistema do Direito, novas tecnologías, globalizaçao e o constitucionalismo contermporaneo: desafios e perspectivas,* Capes/Fapergs/Casa Leira, Brasil.

– FROSINI, V. (1996): "Los derechos humanos en la era tecnológica", en: PÉREZ LUÑO, A. E. (coord.), *Derechos humanos y constitucionalismo ante el tercer milenio*, Madrid: Marcial Pons.

– GARCÍA LÓPEZ, E. (2021): *Estudio de Contextualización ¿Hay derecho a mentir? (La polémica Inmanuel Kant - Benjamin Constant, sobre la existencia de un deber incondicionado de decir la verdad),* Madrid.

– GARCÍA MEXÍA, P. (2017): *La Internet abierta. Retos regulatorios de una Red nacida libre*, REU Ediciones, Madrid.

– KEATS, D. / WITTES, B. (2017): "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity", en: *86 Fordband Law Review*, pp. 401-419.

– KHAN, L. M. (2017): "Amazon´s antitrust paradox", *The Yale Law Journal*, Vol. 126, núm. 3, pp. 710-805.

– MORET MILLÁS, V. y SÁNCHEZ GIL, I. (2022): "A comparative law approach to the regulation of social networking platforms", en: *Revista de las Cortes Generales*, núm. 112, pp. 287-316.

– PAUNER CHULVI, C. (2018): "Noticias falsas y libertad de expresión e información. el control de los contenidos informativos en la Red", en: *Teoría y Realidad Constitucional*, núm. 41, pp. 297-318.

– PIÑAR MAÑAS, J. L. (2018): "Identidad y persona en la sociedad digital", en: DE LA QUADRA-SALCEDO, T. / PIÑAR MAÑAS, J. L. (Dirs.), *Sociedad digital y Derecho*, BOE, Madrid.

– RALLO, A. (2011): "La privacidad en la era digital: el derecho al olvido", en: *Actualidad Jurídica Aranzadi*, 815.

- (2021): "Una nueva generación de derechos digitales", en: *Revista de Estudios Políticos*, 187, pp. 101-135.

– REBOLLO DELGADO, L. / ZAPATERO MARTIN, P. (2019): *Derechos digitales*, UNED/Dykinson, Madrid.

– RODOTÀ, S. (2010): *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid.

- (2018): "Del ser humano al posthumano", en: DE LA QUADRA-SALCEDO, T. / PIÑAR MAÑAS, J. L. (Dirs.), *Sociedad digital y Derecho*, BOE, Madrid, pp. 87-94.

– RODRÍGUEZ-IZQUIERDO, M. (2019): "Las empresas tecnológicas en Internet como agentes de seguridad interpuestos", en: *Revista Española de Derecho Constitucional*, núm. 117, pp. 77-100.

– SÁNCHEZ BARRILAO, J. F. (2016): "El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional", en: *Estudios de Deusto: revista de Derecho Público*, Vol. 64, nº. 2, pp. 225-258.

– SORIANO ARNANZ, A. (2021): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", en: *Revista General de Derecho Administrativo*, nº. 56.

– VÁZQUEZ ALONSO, V. J. (2022): "La censura «privada» de las grandes corporaciones digitales y el nuevo sistema de la libertad de expresión", en: *Teoría & Derecho. Revista De Pensamiento jurídico*, (32), pp. 108-129.

– VILLAVERDE MENÉNDEZ, I. (2007): "Ciberconstitucionalismo, las TIC y los espacios virtuales de los derechos fundamentales", en: *Revista catalana de Dret Public*, núm. 35, pp. 19-42.

– WU, T. (2003): "Network Neutrality, Broadband Discrimination", en: *Journal of Telecommunications and High Technology Law*, Vol. 2, pp. 141 y ss.