ISSN: 2697-1631 | ISSN-e: 2697-2239

Big data, privacidad y mercados digitales: los nuevos desafíos de la regulación en la UE

Análisis desde una perspectiva económica, regulatoria y *antitrust*

Fernando Díez Estella

Profesor titular (acreditado) de Derecho Mercantil. Universidad Villanueva

fdiez@villanueva.edu | https://orcid.org/0000-0002-5011-0051

Alba Ribera Martínez

Doctoranda en Derecho. Universidad Carlos III de Madrid

100454926@alumnos.uc3m.es | https://orcid.org/0000-0002-9152-0030

Este trabajo ha obtenido un **accésit** del **Premio «Estudios Financieros» 2021** en la modalidad de **Derecho Constitucional y Administrativo.**

El jurado ha estado compuesto por: don Juan Antonio Xiol Ríos, doña Lucía Casado Casado, don Gabriel Doménech Pascual, doña Alicia González Alonso, don José Damián Iranzo Cerezo y don Fabio Pascua Mateo.

Los trabajos se presentan con seudónimo y la selección se efectúa garantizando el anonimato de los autores.

Extracto

En fechas recientes el Parlamento Europeo ha emitido un informe favorable al proyecto de la Comisión Europea sobre la estrategia europea de datos. Este nuevo activo estratégico se ha convertido en un elemento esencial, no solo para la actuación de las empresas en el mercado, sino en la vida de los ciudadanos y su forma de relacionarse. En los últimos 15 años los mercados han experimentado vertiginosos cambios derivados, entre otras cosas, de la digitalización de nuevos modelos empresariales y formas de hacer negocio. Pese a que la Unión Europea aspira a la creación de un verdadero *mercado único digital*, lo cierto es que en la actualidad las empresas que dominan el panorama (Google, Facebook, Amazon y Apple) son todas estadounidenses. La ingente acumulación de datos personales que dichas plataformas digitales acumulan y aprovechan comercialmente –el *big data*– plantea indudables riesgos para la protección del derecho fundamental a la protección de los datos personales de los usuarios. En este trabajo se analiza de forma crítica el enfoque comunitario con el que se afronta este escenario, al hilo de operaciones de concentración empresarial o actuaciones de las autoridades de competencia contra dichos gigantes tecnológicos. Se prestará especial atención al contenido constitucional de este derecho, así como al posible solapamiento entre el derecho regulatorio y el administrativo sancionador, en concreto, en el ámbito del derecho de la competencia.

Palabras clave: *big data*; privacidad; mercados digitales; *antitrust*.

Fecha de entrada: 04-05-2021 / Fecha de aceptación: 10-09-2021

Cómo citar: Díez Estella, F. y Ribera Martínez, A. (2022). *Big data*, privacidad y mercados digitales: los nuevos desafíos de la regulación en la UE. (Análisis desde una perspectiva económica, regulatoria y *antitrust*). *Revista CEFLegal*, *252*, 73-104.

Big data, privacy and digital markets: the new regulatory challenge in the EU

Analysis from an economic, regulatory and antitrust perspective

Fernando Díez Estella

Alba Ribera Martínez

Abstract

The European Parliament has recently issued a favourable report on the European Commission's European data strategy draft. This new strategic asset has become an essential element not only for the performance of companies in the market, but also in the lives of citizens and the way they relate to each other. Over the last 15 years, markets have undergone dizzying changes resulting, among other things, from the digitisation of new business models. Although the European Union aspires to the creation of a true *digital single market*, the fact is that today the companies that dominate the landscape (Google, Facebook, Amazon and Apple) are all American. The huge accumulation of personal data that these digital platforms accumulate and commercially exploit –big data– poses unquestionable risks for the protection of the fundamental right to the protection of users' personal data. This paper critically analyses the EU approach to this scenario, in the context of corporate mergers or actions by the competition authorities against these technological giants. Special attention will be paid to the constitutional content of this right, as well as to the possible overlap between regulatory law and administrative sanctioning law, specifically in the field of competition law.

Keywords: big data; privacy; digital markets; antitrust.

Citation: Díez Estella, F. y Ribera Martínez, A. (2022). *Big data*, privacidad y mercados digitales: los nuevos desafíos de la regulación en la UE. (Análisis desde una perspectiva económica, regulatoria y *antitrust*). *Revista CEFLegal*, *252*, 73-104.

Sumario

> Negar un hecho es lo más fácil del mundo. Mucha gente lo hace, pero el hecho sigue siendo un hecho.
>
> **Isaac Asimov**

1. Introducción

En el mes de marzo de 2021 el Parlamento Europeo emitió su informe[1] sobre la Estrategia Europea de Datos, un ambicioso proyecto que la Comisión Europea lleva impulsando fervientemente estos últimos años. En él, se acoge favorablemente esta estrategia, prestando especial atención a que este nuevo activo económico es un requisito para la viabilidad y competitividad de las empresas, y su regulación es un elemento crucial en la construcción de una sociedad de los datos basada en los derechos y valores de la Unión Europea. Además, se señala que para aprovechar todo el potencial de la *data-driven economy*, la futura legislación en esta materia debe diseñarse para facilitar el desarrollo tecnológico, la innovación, el libre acceso a los datos, así como su interoperabilidad, respetando en todo caso los derechos fundamentales de los ciudadanos.

Y es que, en efecto, en los últimos 15 años las empresas líderes mundiales han dejado de ser aquellas multinacionales proveedoras de bienes y servicios tradicionales (ONU, 2019) para dar paso a empresas pertenecientes al mundo digital, que en su mayoría son plataformas digitales (básicamente, las omnicomprensivas Google, Amazon, Facebook y Apple, a las que se suele aludir bajo el acrónimo GAFA). Este cambio, aunque no se ha producido de una forma repentina, ha virado el debate en este ámbito hacia el nivel de intervención necesario de la Administración pública, tanto a nivel nacional como de los organismos comunitarios e internacionales, en el mercado. Frente a este reto, tenemos ante nosotros dos posibles líneas de actuación: por una parte, la regulación económica de este mercado y, por otra, los instrumentos de la normativa *antitrust*, ambos como límite a la libertad de empresa.

En este marco, se plantea la cuestión de si ambas herramientas –puestas en común– atienden suficientemente a los retos planteados por el mundo digital, sobre todo cuando están en juego derechos fundamentales tales como el derecho a la protección de datos reconocido en el ámbito de la Unión Europea en el artículo 8 de la Carta de Derechos Funda-

[1] Resolución de 25 de marzo de 2021, sobre una Estrategia Europea de Datos (2020/2217(INI)).

mentales de la Unión Europea (en adelante, CDFUE), y en el ámbito nacional por derivación del artículo 18.4 de la Constitución española (CE).

En efecto, si algún rasgo podemos decir que caracteriza los tiempos que estamos viviendo, es nuestra creciente sensibilidad hacia nuestros datos personales, y la consiguiente exigencia de que existan leyes e instituciones encargadas de velar por su correcto uso, aparejada de la debida protección de nuestra privacidad. En el ámbito de la Unión Europea esto se ha visto reflejado en la aprobación[2] del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD).

En España, el RGPD provocó un proceso de «actualización» de la normativa en esta materia, que culminó con la promulgación[3] de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPD, en adelante). En fechas muy recientes, se ha vuelto a dar un paso más en esta materia con la apertura de una consulta pública[4] para la elaboración de una Carta de Derechos Digitales.

Sin embargo, la acumulación de información por parte de las GAFA –y no solo– como un recurso más puesto al servicio de la maximización de sus beneficios, a la que nos referiremos en adelante como el fenómeno del *big data*, ha desencadenado una profunda reflexión sobre el papel de la Administración, de las autoridades de competencia y de las autoridades de protección de datos, que expondremos a continuación.

El modelo de negocio impulsado por las plataformas digitales propugna lo que podríamos llamar la «cuasi-apropiación» de cantidades ingentes de datos personales de los ciudadanos, que posteriormente se monetizan a partir de su uso con fines publicitarios. En este trabajo vamos a explorar cuál es la regulación existente del *big data* en relación con la protección del derecho a la privacidad, así como su posible desarrollo en el futuro en el ámbito del derecho administrativo desde la perspectiva de la regulación económica.

En el mismo sentido, expondremos las posibilidades que el derecho de la competencia ofrece, que tienden cada vez más hacia un análisis holístico de los asuntos que se le plantean. En concreto, atenderemos a la reciente operación Google/Fitbit, que ha vuelto a poner sobre la mesa a nivel mundial el debate en torno al *big data* en el ámbito *antitrust* y su posible interrelación con otras disciplinas, de la forma que también lo hicieron otras adquisiciones igualmente mediáticas, tales como Facebook/WhatsApp o Facebook/Instagram.

---

2 DOUE L 119, 4 de mayo de 2016, pp. 1-88 (ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

3 BOE núm. 294, de 6 de diciembre de 2018.

4 Disponible en la web del Ministerio de Asuntos Económicos e Innovación Digital: <https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/SEDIA_Carta_Derechos_Digitales.aspx>.

En este sentido, es evidente que la rápida evolución de los mercados como consecuencia de la digitalización y el surgimiento de nuevos modelos de negocio en el marco de la economía colaborativa ha planteado un debate de la máxima importancia: ¿es el Derecho de la competencia –el encargado de velar por el mantenimiento de un mercado competitivo y de proteger a los consumidores– suficientemente versátil para adaptarse a estas nuevas realidades, o debe actualizarse?

Para hacer frente a este reto, tras varios años de trabajos preparatorios y todo tipo de consultas y documentos de trabajo, el 15 de diciembre de 2020 la Comisión Europea presentó dos propuestas de Reglamentos –la *Digital Markets Act*[5] (en adelante, DMA) y la *Digital Services Act*[6] (en adelante, DSA)– que pretenden reconfigurar la realidad de los servicios y mercados digitales (Díez Estella, 19 de diciembre de 2020; Ibáñez Colomo, 22 de febrero de 2021) en la Unión Europea de los próximos años. Esta propuesta, no exenta de polémica, parte del supuesto de que las grandes plataformas en línea (aunque en ningún momento del texto las menciona, es evidente que está pensando en las GAFA) actúan como *gatekeepers* (Geradin, 18 de febrero de 2021) (guardianes de acceso, en castellano) en los mercados digitales. Frente a ello, se instituye un control *ex ante* frente a su comportamiento en el mercado para garantizar que se comportan de manera leal y equitativa, teniendo en cuenta su predominancia en el mercado.

Tanto la DMA como la DSA forman parte del *Digital Services Act package*[7], que es uno de los ejes de la Estrategia Digital Europea. Esta estrategia, presentada[8] oficialmente en febrero de 2020, tiene como objetivo

> una sociedad europea impulsada por soluciones digitales que sitúan en (un) lugar preferente a las personas, abre nuevas oportunidades para las empresas y da impulso al desarrollo de una tecnología fiable que fomente una sociedad abierta y democrática y una economía dinámica y sostenible,

y consta de dos documentos básicos: la Estrategia Europea de Datos[9] y las opciones estratégicas destinadas a garantizar un desarrollo de la inteligencia artificial[10] centrado en el ser humano.

---

5 Comisión Europea, *A European Strategy for Data,* COM (2020) 842 final. <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en>.

6 COM/2020/825 final.

7 <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.

8 <https://ec.europa.eu/commission/presscorner/detail/es/ip_20_273>.

9 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066>.

10 <https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>.

Así pues, podemos ver que la política impulsada por las autoridades de protección de datos y el derecho *antitrust* están llamados a jugar un papel muy relevante en la configuración, no solo de los mercados europeos y nacionales, sino también de la sociedad en su conjunto. La gran pregunta, sobre la que todavía no se ha llegado a una respuesta unívoca, es si ambos instrumentos han de articularse por separado o de forma complementaria.

Esta será, precisamente, la pregunta a la que se tratará de dar respuesta en este trabajo, y se ilustrará a partir de dos casos emblemáticos, que han puesto de manifiesto la dificultad de encontrar una solución fácil y rápida a este problema: por un lado, el caso *Bundeskartellamt c. Facebook*, impulsado por la autoridad de competencia alemana; por otro, la operación de concentración empresarial Google/Fitbit, analizada a nivel comunitario.

Siguiendo un esquema lineal, definiremos el fenómeno del *big data* y señalaremos las características de las plataformas digitales relevantes de cara a la consideración de esta materia, así como su necesaria puesta en común con la protección de los datos personales (epígrafe 2). Partiendo de lo anterior, apuntaremos las soluciones que ya se han dado hasta ahora en el ámbito del derecho regulatorio y la posibilidad de su interacción con el derecho de la competencia (epígrafe 3). Asimismo, destacaremos aquellas operaciones que en el ámbito *antitrust* han tenido una mayor relevancia, con el fin de extrapolar esas mismas consideraciones a un ámbito más amplio (epígrafe 4). Finalmente, se ofrece un apartado de conclusiones (epígrafe 5).

2. El fenómeno del *big data* confrontado con el derecho a la privacidad

2.1. ¿Qué es el *big data*?

Antes de entrar en el análisis sobre la cuestión esencialmente constitucionalista del derecho a la privacidad, debemos sentar cuál es el enemigo que batir –si es que lo hay–, de las autoridades administrativas. Tal y como expusieron las autoridades alemana y francesa en 2016 (Autorité de la Concurrence y Bundeskartellamt, 2016, pp. 4-5), el fenómeno del *big data* procede de la importancia de los datos, no solo en las plataformas digitales, sino también en todas aquellas empresas presentes en el sector digital, e incluso en los Gobiernos (como hemos visto recientemente con los problemas generados a raíz de la App Radar COVID) (Antón Juárez, 2021, p. 44). No obstante, es verdad que son las plataformas digitales las que han centrado su modelo de negocio sobre la base de la captación y utilización intensiva de datos (Allende Salazar, 2020, p. 6).

El *big data* está compuesto por flujos de información procedentes de una gran cantidad de datos, que van desde los datos personales emitidos por los usuarios de internet, directa o indirectamente, hasta aquellos que conciernen los aspectos del mundo real, como por

ejemplo el clima o la geolocalización. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define el *big data* como un «patrimonio informativo caracterizado por un Volumen, Velocidad y Variedad tan elevados que requieren tecnologías específicas y procedimientos de análisis para su transformación en valor»[11].

Esta definición se basa en el modelo de las tres V, teorizado por Douglas Lanely (6 de febrero de 2001), que describe las principales características del *big data*: volumen, velocidad y variedad, acogida por gran parte de la doctrina (OCDE, 2013, pp. 11 y 12). La característica más importante, y que constituye la cuarta V del *big data*, es su valor, es decir, la capacidad de extraer y transformar estos datos en información económicamente útil casi en tiempo real. Teniendo en cuenta todo lo anterior, podemos afirmar que el *big data* supone la recopilación masiva de datos procedentes de distintas fuentes y tipos, almacenados y procesados adecuadamente a una gran velocidad.

Esta práctica de recopilación, almacenamiento y tratamiento de datos no es especialmente innovadora, puesto que en los mercados tradicionales se suelen procesar igualmente este tipo de datos mediante estudios de mercado y muestreos (Antón Juárez, 2021, pp. 52-53). No obstante, lo que es insólito es la velocidad tanto con la que se generan esos datos por parte de los usuarios como la capacidad de respuesta y procesamiento de los algoritmos a los que se incorporan.

De esta forma, una vez recopilados los datos, estos no otorgan ventaja a aquel que los ha obtenido y no suponen *a priori* amenaza alguna ni para el consumidor ni para la sociedad en general. Algunos autores, tomando la comparación con el proceso productivo, designan a estos datos como el *raw data* (Castillo Parrillas, 2019), que es la materia prima objeto de transformación.

Desde la perspectiva puramente económica, la obtención indiscriminada de datos personales no supone un valor añadido *per se* a la empresa ni tampoco supone una barrera de entrada para otros competidores en el mercado (Sokol y Comerford, 2016). Así, Lambrecht y Tucker (2015) han señalado que «para que se pueda generar una ventaja competitiva significativa, los competidores deben ser completamente incapaces de duplicar los beneficios obtenidos por esta misma estrategia». Según sostienen, las características del *big data* no favorecen que esta premisa se pueda cumplir; existen escasas barreras a la entrada en el mercado digital, ya que los datos almacenados no son exclusivos de aquel que tiene el control sobre ellos –es habitual, en este sentido, el *multi-homing*–, y además tienen un corto plazo de expiración –los datos desfasados no tienen ningún valor, solo son especialmente valiosos aquellos datos agregados, actualizados y diferenciados– (Sokol y Comerford, 2016).

[11] Informe *Big Data: bringing competition policy into the digital era* (2016). <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf>. La OECD retoma la definición adoptada en Mauro, Greco y Grimaldi (2017).

En sentido ligeramente opuesto, otros autores sostienen que el *big data*, especialmente aquel que contiene tendencias de consumo de los usuarios, es susceptible de ser reutilizado, y como tal se trata de un activo no depreciable (Petit *et al.*, 2021). En la sociedad digital, según estos mismos autores, prevalece el enfoque de capacidades, es decir, este tipo de empresas deben adaptarse constantemente a los cambios en el mercado (por ejemplo, frente a la circunstancia de un nuevo entrante en el mercado) para ser capaces de sobrevivir en él ante las incertidumbres que presenta (pp. 20-22).

No obstante, una vez se procesan de una forma eficiente y rápida para refinar y predecir el comportamiento humano con fines comerciales (Krzepicki, Wright y Yun, 2020), por ejemplo, para el lanzamiento de nuevos productos o para impulsar sus tareas de marketing o I+D (OCDE, 2013, pp. 12-13), son susceptibles de ser tratados como un *input* más en el proceso productivo (pp. 14-15) a partir del comportamiento de sus usuarios considerados individualmente (División de Competencia de la OCDE, 2016, pp. 7-8).

Los datos utilizados en este proceso no solo se refieren a los datos personales facilitados de forma voluntaria y consciente (Quadra-Salcedo Fernández del Castillo, 2018, pp. 35 y 36) por el usuario (por ejemplo, su fecha de nacimiento o sexo), sino también a la «huella digital» que este genera en la plataforma (por ejemplo, a través de sus *likes* en Instagram) (Antón Juárez, 2021, p. 42). En este sentido, el *big data* también puede estar integrado por datos no personales, seudonimizados o anonimizados[12]. Estos datos, recopilados y puestos en común, permiten que los sistemas de inteligencia artificial (en adelante, IA) deduzcan patrones y tendencias de consumo (Allende Salazar, 2020, p. 11), creando, por tanto, más valor en el marco del proceso productivo.

El sector digital ha traído consigo la posibilidad de que los operadores en el mercado obtengan una ventaja competitiva en el mercado por esta vía, incorporando el *big data* en su propia actividad, o incluso para vender el *output* generado a terceros, igualmente con fines comerciales (Antón Juárez, 2021, p. 44). Este proceso, aunque aparentemente nocivo, trae consigo un grado de innovación superior y una calidad creciente (Sokol y Comerford, 2016) de los productos y servicios existentes ofrecidos a los usuarios, que, a su misma vez, puede beneficiar a estos y a la sociedad en su conjunto (División de Competencia de la OCDE, 2016, pp. 7-8) (eficiencias, tomando la terminología del derecho de la competencia). Algunos autores insisten en que incluso el modelo de negocio basado exclusivamente en el *big data* ya habría quedado superado actualmente por aquel más bien centrado en la depuración de los sistemas de IA (Allende Salazar, 2020, p. 15).

Prima facie, desde una perspectiva constitucional, nos encontramos con una de las preocupaciones principales en torno al *big data*: su contenido. El Comité Europeo de Protección

[12] Comité Europeo de Protección de Datos. (2014). *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, p. 9. <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf>.

de Datos (CEPD, en adelante) defiende que, comparando los beneficios que las empresas pueden obtener por el uso del *big data*, la intrusión en la privacidad de los consumidores es mucho menos lucrativa y, por lo tanto, mucho menos atractiva. A su misma vez, señala en el mismo informe que en el periodo 2030-2035 la propia noción de datos personales desaparecerá por la facilidad con la que las plataformas digitales podrán identificar –a partir de los datos que han ido recabando sobre ellos– a sus usuarios (Buttarelli, 2017). Incluso hoy en día, un estudio ya demuestra que es posible identificar al 87 % de la población de los Estados Unidos a partir de su código postal, fecha de nacimiento y sexo (Davis y Osoba, 2016), datos que nos podrían parecer a primera vista como «inofensivos».

Por tanto, las plataformas digitales pueden no solo identificar a segmentos o grupos de interés a los que dirigir su actividad de marketing y publicidad, sino también captar y dirigirse directamente a individuos con perfiles concretos (CEPD, 2014, p. 10) con estos mismos fines (lo que se conoce en el sector del marketing como *profiling*). En ocasiones, es posible que el perjudicado por el tratamiento de los datos no sea el mismo sujeto que ha facilitado sus datos personales. Es decir, la tarea de *profiling* que se realice sobre individuos distintos a este, pero con un mismo perfil de consumo, permite a la empresa predecir sus hábitos de consumo y, con base en este, imponerle determinadas decisiones de negocio (Quadra-Salcedo Fernández del Castillo, 2018), como por ejemplo puede suceder en el *scoring* bancario y en el análisis de riesgos que se realiza para la contratación de un seguro (Martínez Martínez, 2018, pp. 264 a 267). Nos encontramos con un proceso que resulta realmente tautológico, es decir, estas herramientas pueden inducir artificialmente el consumo (pp. 267 a 273) del usuario según una identidad y perfil definidos previamente (Piñar Mañas, 2018, pp. 101 a 103).

Por el propio funcionamiento de «caja negra» (Martínez Martínez, 2018, pp. 262 a 264) de este fenómeno, no podemos saber con certeza si realmente los datos personales que los usuarios facilitan a las plataformas digitales serán utilizados en su contra –traducidas en estrategias comerciales agresivas– o si, por el contrario, se enjugarán en un océano de información del que difícilmente podrán ser extraídos una vez incorporados a sistemas de IA.

Lo que sabemos es que, en la actualidad, tanto las plataformas digitales como empresas de otros sectores tienen acceso a estos datos, y pueden utilizarlos para fines completamente distintos a aquellos que motivaron su transferencia en primer lugar (CEPD, 2014, p. 9), de forma contraria a lo contemplado por el RGPD y la LOPD.

2.2. Coste cero para el usuario vs. maximización ¿intrusiva? de los beneficios

Los usuarios de las grandes plataformas digitales disfrutan de sus servicios gratuitamente. A cambio, estas plataformas multilaterales se retroalimentan en función del número de usuarios presentes en ellas. Es decir, cuanto mayor es el número de usuarios en uno de sus lados (por ejemplo, usuarios de Facebook), también mayor es el atractivo para los usuarios

del otro lado de la plataforma (siguiendo el ejemplo, anunciantes en Facebook). Además, a mayor número de usuarios, mayor número de datos que quedarán a disposición de las plataformas para incorporarse y refinar los algoritmos y sistemas de IA que, utilizados eficientemente, producirán unos resultados más relevantes, focalizados y pertinentes (Herrero Suárez, 2018, pp. 666 a 672) para predecir las tendencias de consumo que se pueden dar en relación con los servicios prestados por plataforma (fenómeno conocido como *feedback loop*).

Estos efectos de red, tradicionalmente, generan un interés en los dos lados de la plataforma; la red social contrata sus servicios a los anunciantes, mientras que ofrece a sus usuarios el acceso gratuito a sus servicios. Sin embargo, teniendo en cuenta la consideración del *big data* como un *input* más en el proceso productivo, la transacción plataforma-usuario no se realiza a un precio monetario cero (Allende Salazar, 2020, pp. 4-5), tal y como aparentemente pudiera parecer. Normalmente, el usuario cae en este equívoco influido por la sensación de gratuidad del servicio (CEPD, 2014, p. 32) y consiente, en muchas ocasiones de forma automática, en facilitar uno de los recursos más valiosos para las plataformas digitales: el acceso a sus datos personales. En virtud de ello, la plataforma digital recibe un influjo constante de *big data* con un elevado valor comercial (p. 10), tanto como el usuario permanece y opera en la plataforma digital. De hecho, la OCDE en 2013 ya estimó el valor económico de los datos facilitados por los usuarios a las plataformas digitales en 300.000 millones de euros, y se esperaba que esta cifra se pudiera llegar a triplicar en 2020 (p. 9). En algunas plataformas digitales, esta gratuidad aparente se ve matizada, ya que solamente parte de sus servicios están disponibles para los usuarios gratuitamente, pero en cambio la prestación de sus servicios completa solamente se realiza previo pago (este modelo de negocio se categoriza bajo el concepto de *freemium*) (Petit *et al.*, 2021, pp. 24-25).

Esta relación esencialmente patrimonial entre usuario y plataforma no asegura la privacidad de los datos que se han facilitado, sin perjuicio de que al responsable del tratamiento de datos se le imponen toda una serie de obligaciones para preservar la protección de los datos de su titular (Hernández Corchete, 2018, pp. 293 a 300), a las que atenderemos posteriormente.

2.3. Contenido constitucional del derecho a la protección de datos personales

El ciudadano medio cada día, aún sin hacerlo conscientemente, genera, a través del mero acceso a internet, toda una serie de datos que pueden integrarse en sistemas de IA a una velocidad creciente. En 2014, ya se estimó que en 2020 el almacenamiento digital de datos en línea alcanzara 44 ZB (zettabytes), mientras que en 2009 esta cifra solamente era de 5 ZB (International Data Corporation, 2014, p. 3). A pesar de que este fenómeno es relativamente nuevo, el derecho a la protección de datos personales se ha reconocido en nuestro sistema constitucional, con tal de atajar los riesgos que plantea, desde una perspectiva puramente iuspublicista.

Por una parte, el artículo 8 del CDFUE hace prevalecer el derecho a la protección de los datos de carácter personal, cuyo tratamiento se sujeta a una serie de principios, concretizándose en un gran poder de intervención sobre las modalidades de su tratamiento (Martínez López-Sáez, 2018). Sobre esta base jurídica, en relación con el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE)[13], que exige una regulación a nivel comunitario para la protección de las personas físicas respecto del tratamiento de sus datos de carácter personal, encontramos el RGPD.

Haciendo uso de la competencia específica que se le confiere en el TFUE, el Tribunal de Justicia de la Unión Europea ha ido delimitando su alcance mediante sucesivos pronunciamientos. Ya en 2016, en el asunto *Digital Rights Ireland Ltd.*[14], el tribunal reconoció que la mera conservación de datos de carácter personal supone por sí sola una injerencia tanto en el derecho a la vida privada (*ex* art. 7 CDFUE) como en el derecho a la protección de datos.

En un sentido similar, en el ámbito del Consejo de Europa, la sentencia *Marper c. Reino Unido*[15] indicó que el simple almacenamiento de datos personales equivale a la interferencia con el contenido del artículo 8 del Convenio para la protección de los derechos humanos y las libertades fundamentales[16] (CEDH), que garantiza el derecho al respeto de la vida privada y familiar, integrado igualmente por el derecho a la identidad[17]. Sigue la Gran Sala del Tribunal Europeo de Derechos Humanos (TEDH) que para ponderar si efectivamente se ha producido una violación de dicho precepto, se debe atender al tratamiento de esos datos, tanto respecto de los procesos a los que se iba a someter como a los resultados que se fueran a obtener.

Por su parte, desde la perspectiva nacional, aunque el artículo 18 de la CE no lo reconoce explícitamente, la STC 292/2000[18] sentó que el derecho fundamental a la protección de datos se deriva de este precepto constitucional –apartado cuarto– y que, además, es un derecho fundamental autónomo respecto del derecho a la intimidad –apartado primero–. A pesar de que ambos derechos comparten un fundamento común, que es la dignidad humana, cuyo respeto se reconoce en el artículo 10.1 de la CE (Martínez López-Sáez, 2018, p.

---

13 DOUE C-326, 26 de octubre de 2012, pp. 1-390. (ELI: <http://data.europa.eu/eli/treaty/tfeu_2012/oj>).

14 Sentencia del TJUE (Gran Sala) de 8 de abril de 2014. *Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros*, Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238, apartados 33 a 37.

15 Sentencia del TEDH (Gran Sala) de 4 de diciembre de 2008. *S. y Marper c/ Reino Unido*, 30562/04 y 30566/04, apartado 67.

16 BOE núm. 243, de 10 de octubre de 1979, páginas 23564 a 23570.

17 Sentencias del TEDH (Sección Quinta) de 26 de julio de 2014. *Mennesson c/ Francia*, 65192/11, (ECLI: CE: ECHR:2014:0626JUD006519211) y de 26 de julio de 2014. *Labassee c/ Francia*, 65941/11, (ECLI: CE: ECHR:2014:0626JUD006594111).

18 Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre.

22-24) –que es también premisa axiológica del catálogo de la CDFUE y el CEDH–, el derecho a la protección de datos garantiza un control de la persona sobre ellos, así como el uso o destino que se vaya a realizar a partir de ellos, tal y como ya señaló la STC 94/1998[19]. En el marco de esta interrelación, el Tribunal Supremo[20] ya apuntó que el reconocimiento de la propia identidad es intrínseco al libre desarrollo de la personalidad, *ex* artículo 10.1 de la CE.

Teniendo en cuenta lo anterior, el control real del titular de esos datos personales realmente recae sobre la construcción digital (Martínez López-Sáez, 2018, p. 25) que se pueda realizar de él a partir de sus datos. Dicho control se integra en la esfera de su autorrealización e identidad personal-digital, independientemente de si estos datos personales guardan semblanza alguna con la realidad (Piñar Mañas 2018, pp. 97 a 101).

Cabe incidir en el hecho de que se dispensa protección a todos aquellos datos que permitan la identificación de la persona, y no solamente a aquellos datos más íntimos. El derecho fundamental a la protección de datos alude a toda aquella información que pueda contribuir a identificar a la persona física (Domínguez Álvarez, 2021, pp. 4-5), de forma contraria al principio de igualdad (Quadra-Salcedo Fernández del Castillo, 2018, pp. 56 a 59), y que en este sentido pueda ser utilizada para justificar decisiones públicas o privadas (Troncoso Reigada, 2010). Es decir, «la protección de datos no solo trata sobre la protección de datos, sino principalmente sobre la protección de las personas que hay tras los datos» (Piñar Mañas, 2018, pp. 109 a 111).

Tanto desde una perspectiva puramente nacional como comunitaria, el derecho a la protección de los datos personales colisiona con otros derechos del mismo rango, tales como la libertad de empresa o la propiedad privada, por lo que, para determinar la prevalencia de uno frente a otro, deberá tenerse en cuenta su función social, dado que no existe esa preponderancia de uno sobre el otro (Martínez López-Sáez, 2018, p. 27).

Precisamente por el hecho de que la configuración constitucional del derecho que analizamos no se define constitucionalmente en abstracto (Troncoso Reigada, 2010, p. 53), sino otorgando toda una serie de facultades a su titular –para limitar el uso de la informática, en los términos del propio art. 18.4 CE– nos encontramos con la LOPD, sin perjuicio de que las medidas de injerencia en el derecho fundamental debían, al menos, tener calidad de ley (Hernández Corchete, 2018, pp. 290 a 293).

Dado que el fenómeno del *big data* es completamente heterogéneo, hasta el punto de que no se le puede dar una definición unívoca, sus manifestaciones –que necesariamente resultarán en una injerencia en la vida privada e intimidad del individuo– se pueden dar en el seno de las decisiones de distintas autoridades administrativas. La injerencia que men-

[19] Sentencia del Tribunal Constitucional núm. 94/1998, de 4 de mayo de 1998.

[20] Sentencia del Tribunal Supremo (Sala Primera) de 28 de febrero de 2008.

cionamos se puede dar, tanto en la forma de intercambio de información entre distintas Administraciones[21] como en el tratamiento de todo tipo de información sensible y personal, tales como datos sobre antecedentes policiales[22], médicos[23], sanitarios[24] o laborales[25].

Tan amplia es la heterogeneidad que señalamos que incluso se extiende al ámbito privado, en el que el *big data* se pone al servicio del ánimo de lucro en algunos de los ejemplos que exponemos a continuación. Algunas de estas manifestaciones han sido ya atajadas por la jurisprudencia europea o bien escapan a la normativa actual (Gudín Rodríguez Magariños, 2018).

En este sentido, tenemos el fenómeno de la videovigilancia –incluso mediante el sistema GPS[26]– que en la medida que resulta en la grabación de individuos y en el almacenamiento de estos datos, entra en el ámbito de la protección de los datos personales y supone una injerencia en la vida privada, tal y como lo reconoció el Tribunal de Justicia de la Unión Europea[27]. Tenemos también todo aquello relacionado con el inminente y creciente internet de las cosas –que son toda una serie de dispositivos electrónicos instalados en el hogar y de uso cotidiano, a partir de los que se recopilan datos para diseñar futuras estrategias de ventas o nuevos prototipos, por ejemplo, Alexa de Amazon–, que supone una injerencia en la intimidad clara, en los términos que hemos expuesto anteriormente. Además, nos encontramos igualmente con el fenómeno de la computación en la nube, cuyos riesgos en relación con la protección de datos ya se expusieron en el dictamen del Grupo de Protección de Datos en el seno de la Unión Europea, por ser una herramienta especialmente dañina que facilita la falta de control y transparencia sobre los datos personales[28].

---

21 Sentencia del TJUE (Sala Tercera) de 1 de octubre de 2015, *Smaranda Bara y otros contra Președintele Casei Națională de Asigurări de Sănătate y otros*, asunto C-201/14 (ECLI:EU:C:2015:638), apartados 29 a 46.

22 Sentencia del TEDH (Sección Quinta) de 18 de septiembre de 2014, *Brunet c. Francia*, 21010/10, (ECLI: CE: ECHR:2014:0918JUD002101010).

23 Sentencia del TEDH (Sección Tercera) de 18 de octubre de 2016, *Vukota-Bojic c. Suiza*, 61838/10, (ECLI: CE: ECHR:2016:1018JUD006183810).

24 Sentencia del TEDH (Gran Sala) de 19 de octubre de 2005, *Roche c. Reino Unido*, 32555/96, (ECLI: CE: ECHR:2005:1019JUD003255596).

25 Sentencia del TEDH (Gran Sala) de 3 de abril de 2007, *Copland c. Reino Unido*, 62617/00, (ECLI: CE: ECHR:2007:0403JUD006261700).

26 Sentencia del TEDH (Sección Quinta) de 2 de septiembre de 2010, *Uzun c. Alemania*, 35623/05 (ECLI: CE: ECHR:2010:0902JUD003562305), apartado 46.

27 Sentencia del TJUE (Sala Cuarta) de 11 de diciembre de 2014, *František Ryneš contra Úřad pro ochranu osobních údajů* (C-212/13, ECLI:EU:C:2014:2428), apartados 21 a 35.

28 Grupo de Protección de Datos del Artículo 29 (2012). *Dictamen 05/2012 sobre la computación en nube* (01037/12/ES). <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf>.

Se desprende de todo ello que además de heterogéneo, este es un proceso en construcción, en la medida que se producen lanzamientos constantes en el mercado de nuevas aplicaciones y sistemas tecnológicos (Quadra-Salcedo Fernández del Castillo, 2018, pp. 45 a 51). Por tanto, el derecho a la protección de datos no puede definirse de una forma cerrada, dados los riesgos dinámicos con los que se enfrentan en el día a día. En este sentido, resulta prácticamente inútil que el legislador trate, en sede de regulación, de atajar aisladamente cada manifestación tecnológica (Hernández Corchete, 2018, pp. 273 a 295).

Aun así, los retos que se han planteado en la esfera constitucional –directamente o por derivación del art. 10.1 CE– han descendido a la regulación administrativa, en el ámbito circunscrito a la protección de datos, aislada de otras líneas de actuación, tales como la regulación en el ámbito *antitrust*.

3. Regulación e intervención administrativa sobre el fenómeno del *big data*

3.1. El ámbito de protección de datos desde una perspectiva crítica

El *big data* puesto al servicio de los sistemas de IA, entre otros sistemas técnicos y tecnológicos puestos a disposición de las empresas, forman una cadena –podríamos afirmar de producción– para que las empresas que poseen esos datos puedan generar valor. Frente a ello, el RGPD impone exigencias regulatorias de protección del consumidor, del usuario, así como del ciudadano en general, sobre el responsable del tratamiento de datos, de una forma proactiva (art. 5.2 RGPD) (Hernández Corchete, 2018, pp. 283 a 285).

Frente a la amenaza que suponen las GAFA, residenciadas en su mayoría en los Estados Unidos, y que, hasta hace poco escapaban del alcance del regulador comunitario, el RGPD dota de eficacia extraterritorial (Hernández Corchete, 2018, pp. 288 a 290) a sus disposiciones en relación con el tratamiento de datos desarrollado fuera de las fronteras europeas, con apoyo en la jurisprudencia comunitaria[29] que ya se había pronunciado a favor de esta posición. En este sentido, el RGPD en su artículo 3 garantiza que se produzca este flujo transfronterizo de la regulación, ya que se aplica el principio de territorialidad de apli-

[29] Sentencias del TJUE (Gran Sala) de 8 de abril de 2014. *Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros*, asuntos acumulados C-293/12 y C-594/12 (ECLI:EU:C:2014:238), apartados 33 a 37; de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*, asunto C-131/12 (ECLI:EU:C:2014:317), apartados 45 a 60; y de 6 de octubre de 2015, *Maximillian Schrems contra Data Protection Commissioner*, asunto C-362/14 (ECLI:EU:C:2015:650) apartados 44 y 45.

cación de las normas, que sitúa el centro de gravedad de la relación jurídica en función de la nacionalidad del titular de los datos personales, y no en la nacionalidad del responsable del tratamiento de datos (Hernández Corchete, 2018, pp. 285 a 290). Es decir, si por ejemplo Facebook tiene la intención de tratar los datos personales de ciudadanos alemanes, franceses, italianos o españoles, tendrá que sujetarse tanto a las exigencias del RGPD como a las especificaciones de las legislaciones nacionales correspondientes.

Además, resulta de interés destacar que el RGPD solamente se ocupa de regular aquellos datos personales, es decir, aquellos que pueden identificar directa o indirectamente a una persona física (*ex* art. 4). Con ello, por tanto, se deja fuera al conjunto de datos no personales (considerando 26) que también integran el *big data* y que son susceptibles de generar valor para las empresas tras su procesamiento y refinamiento mediante sistemas de IA. En la propuesta de la DMA, en concreto en su artículo 6 i) se impone a los *gatekeepers* la obligación de no facilitar gratuitamente aquellos datos generados por los propios usuarios de la plataforma, por su indudable valor económico, sin perjuicio de que no se contempla previsión alguna para aquellos supuestos en los que tales datos se transmitan de forma onerosa.

El RGPD establece toda una serie de garantías de cara a la protección del derecho a la protección de los datos personales, como obligaciones que recaen sobre el responsable del tratamiento. En primer lugar, este debe diseñar sus sistemas de IA teniendo en cuenta los riesgos que pueden entrar en colisión con los derechos fundamentales, ya que él es el que los conoce con mayor exactitud (*ex* art. 24 RGPD). En segundo término, debe regir en su actuación tanto el principio de minimización de datos –es decir, que solamente se utilicen datos adecuados, pertinentes y necesarios teniendo en cuenta los fines a los que se van a destinar– (Martínez Martínez, 2018, pp. 275 a 277), como de anonimización (cuando sea posible) en el acceso a los datos personales de sus usuarios (art. 5.1.c RGPD). Alternativamente, la licitud del tratamiento también puede fundamentarse en el consentimiento recabado de la persona que será individualizada mediante el acceso a estos datos (art. 6.1.a RGPD). No obstante, el consentimiento debe ser otorgado de manera afirmativa y tiene que reflejar una manifestación de voluntad libre, específica, informada e inequívoca del sujeto cuyos datos son objeto del tratamiento.

Sin embargo, hasta el momento resulta acuciante la falta de regulación respecto a la integración de los datos personales en los sistemas de IA. Este proceso, en el que se desarrolla la esencia del tratamiento de los datos personales, se encuentra con grandes cortapisas, dado que colisiona con otros derechos igualmente relevantes tales como los derechos de propiedad intelectual. Se podría sostener que este fenómeno, por lo que se refiere a la elaboración de perfiles, ya está contemplado en el artículo 22 del RGPD y el artículo 18 de la LOPD, aunque lo está de forma tenue, puesto que solo se reconoce el derecho del usuario a oponerse a que se tomen decisiones exclusivamente basadas en el *profiling* generado a través de sistemas de IA. Si nos fijamos detenidamente en este extremo de la regulación, solamente se reprocha el hecho de basar las decisiones exclusivamente en el perfil que se ha generado, pero nada impide que sea uno de los elementos a considerar en la toma de

decisiones, sin perjuicio de las buenas prácticas que se recomienden por el CEPD, en virtud del artículo 70.1 f) del RGPD. Otros organismos internacionales como la OCDE[30] y el G-20[31] también impulsan recomendaciones sobre el uso ético de los sistemas de IA (Leslie *et al.*, 2021), aunque siempre en forma de *soft law*, por lo que este extremo del *profiling* sigue quedando huérfano en el plano de la regulación.

En un movimiento que marcará sin duda un hito en esta materia, el pasado 21 de abril de 2021 la Comisión Europea también presentó una propuesta de Reglamento de la IA[32], que incluso prevé un catálogo de sanciones en esta materia. En este sentido, proponemos que, aunque las exigencias impuestas al responsable del tratamiento podrían ser más livianas a aquellas que hemos señalado anteriormente, deberían igualmente asegurar que las empresas diseñen algoritmos adecuados y transparentes. Algunos autores incluso sostienen que el cambio normativo debiera introducir un derecho de los afectados por la decisión de integrar sus datos personales en los algoritmos a conocer su contenido, las variables y ponderación que se realiza de cada una de ellas, así como el tipo y clase de datos al que se le ha dado acceso al sistema de IA (Quadra-Salcedo Fernández del Castillo, 2018, pp. 44 y 45).

Siguiendo con el análisis crítico de la normativa de protección de datos actual, el artículo 6.1 f) del RGPD contempla los tratamientos de datos personales ligados a actividades de interés privado desvinculados de aquellos motivados en el interés público, ya que persiguen finalidades distintas. Mientras que respecto de estos últimos el RGPD se remite al legislador nacional para fijar cuáles son tales fines de interés público, los primeros se admiten incluso sin el consentimiento del titular de los datos, siempre que sean necesarios para la satisfacción de estos intereses y con el límite de que no prevalezcan los derechos fundamentales apuntados anteriormente que podrían quedar afectados. Por tanto, tenemos que la legislación nacional de los Estados miembros no puede determinar qué intereses privados son más legítimos que otros, sino que este interés, tal y como queda definido en el RGPD, ya es título habilitante del tratamiento. En este sentido, el legislador comunitario se decanta por una mayor uniformización del sistema de protección de datos personales, con el fin de potenciar una mayor competencia entre el tratamiento de datos destinado a la actividad privada de las empresas en el mercado. Es decir, como contemplamos en otras ocasiones, desde la esfera comunitaria se persigue idéntico objetivo: la consecución del mercado interior (Hernández Corchete, 2018, pp. 285 a 292). Todo este régimen regulatorio compele al responsable del tratamiento, pero de forma moderada, por cuanto que contiene una definición abierta de las circunstancias que podrían conducir a una multa sancionadora, sin que

---

30 Recommendation of the Council on Artificial Intelligence (OECD/Legal/0049), 22 de mayo de 2019. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

31 G20 Ministerial Statement on Trade and Digital Economy, June 2019. <https://www.mofa.go.jp/files/000486596.pdf>.

32 Propuesta de Reglamento del Parlamento Europeo y del Consejo, COM(2021) 206 final. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence>.

necesariamente su incumplimiento conlleve a una reacción sancionadora inmediata como consecuencia del incumplimiento.

Por tanto, al haber realizado este análisis crítico de la regulación, se evidencia que el RPGD y su posterior plasmación en la LOPD dejan grandes lagunas exentas de regulación por las que se puedan colar flagrantes infracciones del derecho fundamental a la protección de datos, que podrían colmarse con la interacción con otras ramas jurídicas tales como el derecho *antitrust*.

3.2. Solapamientos entre el derecho regulatorio y el derecho de la competencia: evolución y posibles soluciones

Los datos de los usuarios, principalmente de las plataformas digitales, además de un «rasgo» de la personalidad que merecen la protección constitucional a la que hemos hecho referencia en el apartado anterior, representan también un insumo que, tratados conjuntamente mediante sistemas de IA generan un *output* de gran valor económico. Aun siendo cierta esta premisa que justifica la consideración del *big data* como un elemento más a tener en cuenta en los análisis de las autoridades de competencia (Ferrer y Pol, 2020), tal y como señaló el CEPD en 2014 (CEPD, 2014, pp. 6-7), esta materia es tratada tanto por las autoridades de competencia como las agencias de protección de datos de forma fragmentaria (Quadra-Salcedo Fernández del Castillo, 2018, pp. 63- 65).

Es decir, existe un curso paralelo entre las líneas de actuación que utilizan ambas para atajar una misma preocupación (Sokol y Comerford, 2016): hasta qué punto el *big data* es nocivo para los usuarios de las plataformas digitales y, a grandes rasgos, para la sociedad en su conjunto. Ohlhausen y Okuliar (2015), en un intento de sistematizar este fenómeno fragmentario, indican las razones por las que estas dos líneas de actuación discurren hasta el momento de forma paralela, y señalan en qué manera deberían interactuar ambas ramas del derecho. Su análisis parte de que los datos personales se han convertido crecientemente en un *input* empresarial, pero resulta complicado asociarles un valor concreto en relación con el precio del servicio, por lo que desde la perspectiva del derecho de la competencia resulta metodológicamente complicado encajar este elemento en sus análisis. Asimismo, señalan que resulta empíricamente impreciso forzar las herramientas *antitrust* para que encajen con los riesgos generados por el *big data* en sede de la protección de los datos de los usuarios. Según lo que sostienen, el *big data* tratado mediante los sistemas de IA oportunos conlleva a una mayor innovación y a la prestación de un servicio de una mayor calidad, desde una perspectiva puramente económica.

Por tanto, todos los análisis de competencia que se centren en determinar el daño anticompetitivo del *big data* como fenómeno se asientan sobre una apreciación subjetiva del daño anticompetitivo y en modelos económicos excesivamente simplistas, y que en ocasiones adolecen de un enfoque dinámico, prestando solo atención a la perspectiva estática de los mercados digitales, lo cual es ciertamente reduccionista y miope (Petit *et al.*, 2021, pp. 4-6).

Es decir, las autoridades de competencia buscarían imponer una presunción de culpabilidad por virtud de la identidad de los supuestos infractores –principalmente los GAFA– sin atender a la realidad fáctica, que demuestra que el *big data* es susceptible de crear grandes beneficios a los propios usuarios como a la sociedad en su conjunto. En este mismo sentido, se detecta una tendencia más acusada por realizar apreciaciones subjetivas desde la perspectiva del derecho de la competencia, como se ha puesto de manifiesto a través de los instrumentos propuestos por la Comisión Europea para combatir a aquellos operadores prevalentes en el mercado o *gatekeepers*, a través de las obligaciones que se les imponen en la DMA.

Adoptando esta misma perspectiva, cuando las autoridades de competencia han analizado los asuntos que se le presentan, tradicionalmente han dejado fuera todas las consideraciones relacionadas con el derecho a la protección de los datos personales. De esta forma, en sus conclusiones siempre omiten cualquier consideración a las normas específicas que regulan esta materia, a salvo de lo que expresen las autoridades de protección de datos competentes. Esta postura resulta cuando menos llamativa, puesto que una de las finalidades del derecho de la competencia es precisamente asegurar la competencia en el mercado para que sus resultados repercutan directamente en un mayor bienestar social. Por lo que se refleja de su actuación, por tanto, las autoridades de competencia no consideran que la protección del derecho a la protección de los datos personales se integre dentro de esta esfera de la protección del bienestar social que se persigue.

Este solapamiento entre las consideraciones de privacidad y las consideraciones *antitrust* ha seguido una clara evolución en la práctica decisoria de la Comisión Europea, en la que el papel de los datos en el control de concentraciones ha ido en un patente *in crescendo*. Así, en la operación TomTom/TeleAtlas, aprobada[33] en 2008, se reconocieron –por primera vez– los datos como un parámetro de competencia, pero no se consideró su naturaleza personal ni la aplicación de la normativa de protección de datos. Ese mismo año, la operación[34] Google/DoubleClick se aprobó «sin perjuicio de las obligaciones impuestas a las partes por la legislación comunitaria en relación con la protección de las personas y la protección de la privacidad con respecto al tratamiento de datos personales»[35]. Idéntica postura se adoptó respecto de la operación Facebook/WhatsApp, aprobada[36] en 2014, y en la que hay una cierta sensación[37] de que la Comisión Europea pecó de no haber dado a los datos y las consideraciones de privacidad la importancia que tenían (relegando[38] esa valoración a las autoridades de protección de datos).

---

33 Decisión de la Comisión Europea de 14 de mayo de 2008 (COMP/M.4854 - *TomTom/TeleAtlas*).

34 Decisión de la Comisión Europea de 11 de marzo de 2008 (COMP/M.4731 - *Google/DoubleClick*).

35 *Ibidem*, párrafo núm. 368.

36 Decisión de la Comisión Europea de 13 de octubre de 2014 (COMP/M.7217 - *Facebook/WhatsApp*).

37 *Vid.*, entre otros, Allende Salazar (2020, p. 425).

38 *Ibidem*, párrafo núm. 164.

No fue hasta el 2016, con la operación[39] Microsoft/Linkedin en que se sentaron las bases para un cambio de paradigma. En ella, la autoridad comunitaria examinó por primera vez en qué medida la pérdida de control sobre los datos personales de una empresa en favor de la otra y la lesión de la privacidad de sus usuarios podría suponer un daño competitivo. De hecho, se tuvieron en cuenta las propias limitaciones que impondría el RGPD en el futuro cercano para descartar que Microsoft tuviera la posibilidad de transmitir y tratar datos personales con fines esencialmente comerciales. Como es lógico en este tipo de supuestos, la Comisión Europea tuvo en cuenta que el bienestar del consumidor podría verse afectado por la acumulación de *big data* por las empresas que se concentran, en concreto porque podrían darse decrementos en la calidad de los productos y en la innovación razonablemente prevista para las empresas competidoras en el mercado (Herrero Suárez, 2018, pp. 673 a 680). Este nuevo enfoque se vio confirmado en 2018, en idénticos términos y con las mismas referencias explícitas a la normativa de protección de datos y el RGPD, al aprobar la operación[40] Apple/Shazam.

En una reciente intervención pública[41], la comisaria Vestager advirtió a la compañía Apple de que los cambios que había introducido en su política de privacidad –encaminada a proteger más a los usuarios– no podía otorgar una ventaja injustificada a sus aplicaciones frente a las de sus competidores, en cuyo caso consideraría una infracción de la normativa de competencia. Sin llegar ninguno de ellos a culminar en sanción, esta misma práctica ha sido objeto de expedientes *antitrust* por parte de las autoridades de competencia italiana[42], inglesa[43] y francesa[44].

¿Cómo establecer el adecuado equilibrio entre protección de la privacidad y protección de la competencia? En el marco de este binomio, y la convergencia entre ambos bienes jurídicos, examinaremos casuísticamente aquellos otros hitos que se han dado en la práctica decisoria de las autoridades *antitrust* como intentos por aproximar ambas materias, sin necesidad de incurrir en premisas axiológicas rotundas sobre el daño causado por el *big data.*

4. La práctica ante las autoridades de competencia

Como paso previo a realizar este análisis, señalaremos, siquiera brevemente, cuáles son las tres grandes líneas de intervención del derecho de la competencia sobre la actividad de los operadores en el mercado. Por una parte, tenemos la actuación estrictamente sancio-

39 Decisión de la Comisión Europea de 6 de diciembre de 2016 (COMP/M.8124 - *Microsoft/Linkedin*).

40 Decisión de la Comisión Europea de 6 de septiembre de 2018 (COMP/M.8788 - *Apple/Shazam*).

41 <https://www.reuters.com/article/idUSL1N2KE243>.

42 Nota de prensa (en inglés): <https://en.agcm.it/en/media/press-releases/2020/10/A542>.

43 Resumen del caso en: <https://www.gov.uk/cma-cases/investigation-into-apple-appstore>.

44 Nota de prensa (en inglés): <https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-framework-autorite-does-not-issue>.

nadora que atiende a la conducta de los competidores en el mercado, ya sea a través de acuerdos entre ellos –prácticas colusorias–, prohibidos por el artículo 101 del TFUE y por el artículo 1 de la Ley 15/2007, de 3 de julio, de defensa de la competencia (en adelante, LDC), o bien porque uno de ellos se prevalece de su posición de dominio en el mercado –abuso de posición dominante–, prohibido por el artículo 102 del TFUE y el artículo 2 de la LDC.

Por otra parte, nos encontramos con la intervención de la autoridad de competencia en las operaciones de adquisición y fusión entre empresas, es decir, las concentraciones entre empresas. Estas últimas, sobre las que nos centramos en su desarrollo más reciente en relación con el tratamiento de datos personales, están regidas principalmente por el Reglamento (CE) n.º 139/2004 del Consejo, de 20 de enero de 2004, sobre el control de las concentraciones entre empresas[45].

Las autoridades de competencia realizan un análisis prospectivo para determinar cuáles serán los efectos que generarán estas operaciones para asegurar el correcto funcionamiento del proceso competitivo en el futuro. De esta forma, se trata de determinar el daño competitivo que se generará en el mercado por la eliminación de al menos uno de los competidores del mercado (uno de ellos en caso de absorción o ambos en caso de constituir una *joint-venture*). Como es lógico, solamente las operaciones más relevantes del mercado, sujetas a determinados umbrales fijados en función del volumen de negocios de las empresas concurrentes, son analizadas por las autoridades de competencia. Una vez determinado que procede este análisis, las concentraciones pueden ser aprobadas en primera fase (porque la operación no plantee problema alguno para la competencia o porque se concluyan compromisos con la autoridad suficientes para atender los riesgos anticompetitivos de esta), o bien en segunda fase, en la que se analizan aquellas operaciones que ocasionan unos problemas de competencia más complejos y que requieren de un análisis detallado y detenido de la autoridad.

4.1. La operación de concentración Google/Fitbit

En una afirmación que, con el tiempo, ha ido cobrando cada vez más relevancia, señaló hace pocos años la actual vicepresidenta de la UE que «a medida que los datos sean más importantes para la competencia, tendremos que examinar más detenidamente aquellas operaciones que impliquen la acumulación de grandes volúmenes de datos»[46].

En efecto, ante la propuesta de adquisición de Fitbit por parte de Google[47], cuyo análisis recayó en la Comisión Europea, la autoridad manifestó en primera fase su preocupa-

[45] DOUE L 024, 29 de enero de 2004, p. 1-22. (ELI: <http://data.europa.eu/eli/reg/2004/139/oj>).

[46] M. Vestager, comisaria de la Competencia en la Unión Europea (Comisión Europea). Speech: «Clearing the path for Innovation», Web Summit, Lisboa (Portugal), 7 de noviembre de 2017.

[47] Adquisición anunciada en noviembre de 2019. <https://blog.google/products/devices-services/agreement-with-fitbit/>.

ción por el posible impacto de la operación, teniendo en cuenta la posición dominante que Google ya ostentaba en el mercado de las búsquedas online en el mercado interior común. La entidad resultante de la fusión tendría acceso al *big data* de Fitbit, que contiene sobre todo datos sobre la salud de sus usuarios, puesto que sus dispositivos recopilan información sobre el latido de su corazón, su ingesta de calorías diaria, las distancias recorridas o sus hábitos de sueño, entre otros.

La Comisión temía que Google pudiera utilizar estos datos para diferenciarse de sus competidores, tanto en los mercados de la publicidad en línea como en el mercado de los servicios de *ad tech* (herramientas analíticas y digitales utilizadas para facilitar la venta y compra programática de publicidad digital). Paralelamente, los operadores del mercado consultados en la operación, autoridades de protección de datos y autoridades de competencia[48] ya habían señalado que la operación planteaba serios problemas en relación con la pérdida de control por parte de los consumidores sobre sus datos sanitarios. De ahí que la adquisición de Fitbit aumentaría las barreras de entrada en el mercado, causando un perjuicio a los anunciantes, que se enfrentarían a precios más altos y menos competitivos.

Teniendo en cuenta todo ello, la Comisión Europea dio paso a la segunda fase de la evaluación[49]. La preocupación de la autoridad comunitaria era que Google pudiese afianzar aún más su posición en el mercado de la publicidad en línea a través del acceso a la base de datos de Fitbit. En efecto, al igual que en otras operaciones de concentración similares en el ámbito de los mercados digitales, se tomó en cuenta si la recopilación de los datos de ambas empresas podría ser utilizada para mejorar el servicio de publicidad online de Google.

En este sentido, la Comisaria Vestager afirmó[50] que la investigación pretendía «garantizar que el control por parte de Google de los datos recogidos a través de los dispositivos wearables, como resultado de la transacción, no distorsione la competencia». Esto es así, ya que el uso de estos dispositivos por parte de los consumidores europeos parece que se irá intensificando en el futuro próximo, aumentando por tanto los datos a disposición de Google, lo que a su misma vez podrá resultar en que este trate datos masivamente para su propio beneficio. Por su parte, el CEPD ya había expresado su inquietud en relación con la privacidad de los datos de los usuarios de Fitbit y con las posibles infracciones del RGPD en las que Google podría incurrir combinando y acumulando los datos sanitarios de los usuarios de Fitbit[51].

---

48 En particular, la autoridad australiana de competencia había indicado que existe una fuerte interacción entre los datos y la competencia. <https://www.accc.gov.au/public-registers/mergers-registers/public-informal-merger-reviews/google-llc-proposed-acquisition-of-fitbit-inc>.

49 Comunicado de prensa de la Comisión Europea, de 4 agosto de 2020, ref. IP/20/1446. <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1446>.

50 *Ibidem*.

51 CEPD, comunicado de prensa del 20 febrero de 2020. <https://edpb.europa.eu/news/news/2020/eighteenth-edpb-plenary-session_en>.

Una vez concluidas sus investigaciones, la Comisión Europea autorizó la operación, condicionada al cumplimiento por parte de Google de un paquete de compromisos durante 10 años, bajo la supervisión de un comisario. Según estos compromisos, Google no podrá utilizar los datos sanitarios adquiridos a través de Fitbit para mejorar la publicidad dirigida al ámbito del Espacio Económico Europeo (EEE). Además, tendrá que almacenar separadamente los datos procedentes del *big data* de Fitbit y los datos relativos a los usuarios de Google. En el comunicado de prensa en el que hizo pública su decisión, la Comisión Europea reafirma que la operación se autoriza sin perjuicio de la obligación de Google de cumplir con el RGPD en el tratamiento de los datos sanitarios de los consumidores, puesto que ya existen herramientas regulatorias específicas para abordarlas. En estos términos se expuso que:

> la investigación de la Comisión Europea determinó que Google deberá acreditar la conformidad de la operación de acuerdo con las disposiciones y principios del RGPD, que incluso permitirían prohibir el tratamiento de los datos sanitarios obtenidos, salvo que los usuarios consientan expresamente a que se realice dicho tratamiento. *Estas consideraciones no se pueden realizar en el ámbito del control de concentraciones*, dado que hay herramientas regulatorias m*ás adecuadas* para determinar la conformidad de la conducta de Google con el RGPD[52].

Aunque soterradamente la Comisión Europea *de facto* entró a analizar las cuestiones relativas a la protección de los datos personales de los usuarios, tanto de Google como de Fitbit, insiste en que no es materia objeto del derecho de la competencia.

Naturalmente, este enfoque tan favorable a la operación, que la considera exenta de riesgos para el mercado y para los consumidores, no es compartida por todos. Sirva, como botón de muestra el informe[53] publicado por el Centre for Economic Policy Research, enormemente crítico con la autorización de esta operación de concentración, ya que, en su opinión, supone un daño directo a los consumidores, un fortalecimiento de la ya dominante y excluyente posición de Google en el mercado de los datos (en este caso, además, especialmente sensibles, por tratarse de datos sanitarios), y una operación cuya única finalidad es monetizar dichos datos.

Este documento, además de proponer una serie de teorías del daño muy sugerentes para abordar los problemas que estamos analizando en estas páginas (relativas a la acumulación de datos, la discriminación monopolística, etc.) señala, en frontal oposición a las palabras que acabamos de citar de la comisaria Vestager, que

---

52 Comisión Europea, comunicado de prensa IP 20/2484 (la cursiva es nuestra).

53 CEPR Policy Insight núm. 107, September 2020: Google/Fitbit will monetise health data and harm consumers. <https://cepr.org/sites/default/files/policy_insights/PolicyInsight107.pdf>.

> los problemas que la operación plantea respecto a la privacidad de los datos amplifican nuestra preocupación. Las disposiciones del RGPD tienen sus limitaciones regulatorias, pero el incumplimiento del derecho fundamental a la protección de datos personales está especialmente relacionado, a su misma vez, con el poder de mercado de Google.

Luego, las cuestiones relativas a la privacidad… ¡sí son una cuestión que atañe a la política de competencia[54]!

4.2. El caso *Bundeskartellamt c. Facebook*

Como venimos señalando, la incorporación de los datos personales como *activo* estratégico en los modelos de negocio de las empresas ha supuesto, en la práctica, que la normativa de protección de datos interaccione con la política de competencia. En particular, en aquellas estrategias comerciales consistentes en recabar ingentes cantidades de datos de los usuarios de plataformas digitales de forma desproporcionada en relación con la actividad que presta. A este respecto, hay un amplio debate sobre si la imposición de estos términos y condiciones (TyC) por parte de las plataformas digitales puede considerarse como una cláusula abusiva, o si estas conductas constituyen una violación del RGPD, en particular por ser contrarias al principio de minimización de los datos.

A este respecto, el que hasta la fecha constituye sin duda el caso más paradigmático para ilustrar esta problemática es el que ha llevado a cabo la autoridad de competencia alemana, la Federal Cartel Office (FCO) o Bundeskartellamt, no por vía de control de las concentraciones empresariales, como hemos expuesto en la operación Google/Fitbit, sino por vía de la prohibición de abuso de posición dominante del artículo 102 del TFUE.

La FCO comenzó a investigar en 2016 si dichas conductas, llevadas a cabo por una empresa en posición dominante en el mercado de las redes sociales como Facebook, podrían constituir un abuso de dominio (Volmara y Helmdachb, 2018), consistente en la imposición de cláusulas contractuales abusivas en sus TyC a sus usuarios. Tras analizar detalladamente los TyC de los servicios ofrecidos por Facebook, concluyó[55] que el tratamiento integral de dichos datos personales infringía el RGPD.

Resolviendo el recurso interpuesto por Facebook, el Tribunal Superior Regional de Düsseldorf (OLG) suspendió la decisión de la FCO, al apreciar que la teoría del daño cons-

---

[54] Y así se manifiesta desde la doctrina más autorizada. *Vid.*, entre otros: Caffarra y Valetti (4 de marzo de 2020).

[55] *Facebook c. Bundeskartellamt,* asunto B6-22/16, case summary, 15 de febrero 2019, p. 4. <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3>.

truida para determinar el abuso de dominio había sido incorrecta. Señala el OLG que «el tratamiento de datos por parte de Facebook [...] no da lugar a ningún daño competitivo relevante ni a ninguna evolución indeseable de la competencia»[56]. El OLG señala que la conducta prohibida y sancionada por la FCO no da lugar a un resultado anticompetitivo, y que la recopilación y el tratamiento de los datos de los usuarios de Facebook no perjudica al mercado, dado que los datos en cuestión pueden duplicarse sin dificultades y ponerse a disposición de cualquier tercero, incluidos los competidores de Facebook en el mercado de las redes sociales.

El OLG cuestiona la teoría del daño construida en torno a la normativa de protección de datos, dado que no aprecia que se haya producido una pérdida de control por parte de los usuarios de sus datos personales. Esto es así, ya que los usuarios podían elegir sobre el tratamiento de sus datos, es decir, si lo autorizan o no. Si bien es cierto que Facebook condicionaba la prestación de sus servicios al consentimiento del usuario en sus TyC mediante el sistema *opt-in*, este era libre de no aceptar la política de privacidad y no registrarse en la red social.

Recurridas las conclusiones alcanzadas por el OLG, en junio de 2020 el Tribunal Federal de Justicia alemán revocó[57] dicha decisión, considerando que la recopilación de datos de los usuarios por parte de Facebook se realizó sin el consentimiento necesario y que por tanto constituye un abuso de posición de dominio.

4.3. La perspectiva estadounidense: el DOJ y la FTC contra Google y Facebook

No podemos olvidar, al realizar esta sistemática de los casos más relevantes que en los últimos años se han pronunciado sobre el impacto competitivo del *big data*, la referencia a la cuestión en el sistema jurídico de los Estados Unidos. No en vano, fue allí donde nació el derecho *antitrust* (mediante la *Sherman Act* aprobada en 1890) y las GAFA están residenciadas en suelo estadounidense, a pesar de que han expandido mundialmente su modelo de negocio. De hecho, en sede estadounidense se han incoado sendos expedientes contra Google y Amazon, exactamente por la misma práctica de abuso de posición dominante (si utilizamos sus términos, *monopolization*, sancionada por la sección 2.ª de la *Sherman Act*).

---

[56] *OLG, Facebook*, asunto VI-Kart 1/19, p. 6. La traducción al español ha sido realizada a partir de del texto en inglés de la decisión del D'Kart Antitrust Blog. <https://www.d-kart.de/wp-content/uploads/2019/08/OLG-D%C3%BCsseldorf-*Facebook*-2019-English-1.pdf> (traducción no oficial).

[57] Tribunal Federal de Justicia, comunicado de prensa núm. 080/2020, 23 de junio de 2020. <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf?__blob=publicationFile&v=2>.

El punto de partida de la investigación de ambas conductas es el informe del House Judiciary Committee Antitrust Subcommittee, publicado en octubre de 2020, que contiene una serie de recomendaciones que, para algunos analistas (López-Galdós, 6 de octubre de 2020), versan en conductas que solo resultarían perjudiciales para los consumidores. El informe asume que las GAFA (y solo ellas) han incurrido en prácticas anticompetitivas, como el autofavorecimiento de sus productos (es decir, aprovechar su condición de *gatekeepers* para favorecer discriminatoriamente a sus propios productos frente a aquellos de sus competidores), la adquisición de empresas de nueva creación para eliminar su capacidad competitiva del mercado (*killer acquisitions*), el uso indebido de los datos recopilados y la creación de barreras de entrada en el mercado. Para resolver estos problemas de competencia que en apariencia atañen exclusivamente a las GAFA, el informe propone revisar el sistema de competencia y la jurisprudencia existentes frente a la inmunidad antimonopolio de estas grandes empresas tecnológicas, ya que las autoridades de competencia en los Estados Unidos no han podido frenar estas prácticas anticompetitivas hasta el momento, también por una falta acuciante de recursos materiales y humanos.

Poco después de la publicación de este informe, el Departamento de Justicia de los Estados Unidos (DOJ, en adelante) presentó una demanda[58] contra Alphabet Inc., la empresa matriz de Google, por *monopolización* (en términos comunitarios, abuso de posición dominante). El núcleo de la demanda estriba en los contratos de distribución[59] exclusiva, consistentes en el favorecimiento de su propio buscador, firmados tanto con Apple respecto de sus dispositivos iOS como con aquellos de su propio sistema operativo Android. Estos pactos, según lo planteado por el DOJ, otorgarían una ventaja injustificada a Google e impedirían la entrada al mercado de sus competidores, afianzando así su situación cuasimonopolista (recordemos que Google tiene, en los Estados Unidos, una cuota en torno al 90 % en el mercado de las búsquedas *online*).

El punto de partida de la demanda del DOJ, y aquí es patente el paralelismo con el planteamiento asumido por la Comisión Europea en la DMA, es que Google es un *gatekeeper* monopolista en el marco de internet. En la línea que esbozamos anteriormente, el DOJ parte de que Google ostenta un «poder monopolístico», tanto en el mercado de búsquedas generales en internet como en el de la publicidad *online* derivada de búsquedas, así como en el mercado de los anuncios de texto en los Estados Unidos. Es decir, es un operador dominante en todos estos mercados. Por tanto, a través de los contratos de distribución exclusiva que apuntábamos, el DOJ señala que «al restringir la competencia en el mercado de las búsquedas generales, la conducta de Google ha perjudicado a los consumidores, reduciendo la calidad de estos servicios […], reduciendo su capacidad de elección e impidiendo la innovación». Natu-

58 <https://www.justice.gov/opa/press-release/file/1328941/download>.

59 Esta parte del expediente es exactamente igual al seguido en la Unión Europea años antes: Decisión de la Comisión Europea de 18 de julio de 2018 en el asunto AT.40099 - *Google Android*. <https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099>.

ralmente, la empresa se aprestó a calificar la demanda como infundada (Waler, 20 de octubre de 2020), y que no beneficiaba a los consumidores, y ha sido ya objeto de múltiples análisis[60].

A diferencia de la Unión Europea, que lleva años persiguiendo y sancionando este tipo de conductas presuntamente anticompetitivas llevadas a cabo por las GAFA, la demanda del DOJ contra Google es la primera gran ofensiva de este tipo en un par de décadas, y sin duda ha abierto la veda a otras posteriores, como la presentada[61] contra Facebook pocos días después, esta vez por la Federal Trade Commission (FTC).

En la denuncia planteada por la FTC, esta afirma que Facebook ha mantenido una posición dominante en el mercado de las redes sociales personales en Estados Unidos desde 2011, con una cuota de mercado de más del 60 %. Cabe reseñar que el mercado de las redes sociales tiene barreras de entrada especialmente altas, dados sus efectos de red (una red se vuelve más atractiva a medida que un mayor número de nuestros amigos y familiares se unen a ella, por lo que resultará necesariamente menos atractivo este mercado para nuevos entrantes a él). A continuación, la FTC describe la forma en la que compite la red social en el mercado; por ejemplo, son especialmente relevantes en el modelo de negocio de Facebook la experiencia del usuario, la funcionalidad y las opciones de protección de la privacidad. El modelo de negocio de Facebook se centra en la publicidad basada en los datos personales de los usuarios que recoge la compañía y que modela su experiencia en la red social, prácticamente de forma única. De hecho, la empresa admite que obtiene prácticamente «todos sus ingresos de la venta de espacios publicitarios a los anunciantes». En 2019 Facebook generó casi 70.000 millones de dólares por el cobro a sus anunciantes por el acceso a Facebook e Instagram.

Partiendo de esta posición dominante de Facebook en el mercado de las redes sociales personales, la FTC denuncia su estrategia anticompetitiva, consistente en la adquisición de dos de sus competidores potenciales; de Instagram en 2012 y de WhatsApp en 2014. Ambas redes sociales estaban llamadas a ocupar un papel muy relevante en este mercado, por lo que Facebook las identificó como una amenaza y las adquirió para evitar tener que competir con ellas en un futuro próximo. La FTC, además, subraya que, durante este periodo, ambas redes sociales podrían haber ganado poder de mercado, a pesar de los efectos de red que *Facebook* poseía por su propia dimensión y, por lo tanto, las subsume en la lógica de las *killer acquisitions*. No obstante, cabe señalar que, desde una perspectiva puramente empírica, la capitalización del 75 % de este tipo de inversiones se realizan con éxito por vía de absorción, como sucede en el supuesto que nos atañe, y no vía salida a Bolsa (Petit *et al.*, 2021, pp. 42-45).

Es especialmente clamoroso, en la demanda de la FTC, la inclusión de un correo electrónico de 2008 de Mark Zuckerberg en el que afirmaba que «es mejor comprar que competir».

---

60 *Vid*., entre otros, Geradin (21 de octubre de 2020).

61 <https://www.ftc.gov/system/files/documents/cases/1910134fbcomplaint.pdf>.

El correo electrónico es anterior a ambas compras, lo que evidencia que ambos movimientos eran parte de una estrategia anticompetitiva. Por último, como cierre de esta estrategia, además, Facebook restringió el acceso de terceros, en su mayoría desarrolladores de *software* a las aplicaciones del grupo. Según la FTC, Facebook ha estado aplicando condiciones anticompetitivas en el acceso a las interconexiones de su plataforma (como la aplicación de interfaces de programación que están disponibles para las aplicaciones de software de terceros) y se refiere para ello a documentos internos de Facebook (principalmente correos electrónicos de altos ejecutivos, incluyendo a Mark Zuckerberg, con afirmaciones del estilo de «Instagram se ha convertido en un competidor grande y viable para nosotros en lo que respecta a las fotos móviles» o «[WhatsApp] es la mayor amenaza para nuestro producto que he visto en mis 5 años aquí en Facebook....»).

Parece, por tanto, que la estrategia comercial que se le achaca a Facebook causó un daño real, tanto a los consumidores, al privarles de la posibilidad de acceder a redes sociales alternativas, como a los anunciantes, por la pérdida de oportunidades de negocio, al subsumirse las tres redes sociales bajo la misma matriz de Facebook. En consecuencia, y siempre según la FTC, los usuarios de las redes sociales personales en los Estados Unidos se han visto privados de las eficiencias generadas por la competencia en ese mercado, tales como la innovación, las mejoras de la calidad y las opciones de los consumidores.

De todo ello se desprende que el *big data* y las formas en que se utiliza en el modelo de negocio puede influir en el daño competitivo que se genere. Como hemos comprobado analizando algunos de los principales casos analizados por las autoridades de competencia comunitaria, alemana y estadounidense, no se trata de una «caza de brujas» a las GAFA por el simple hecho de ser *gatekeepers* en el mercado, sino que advertimos un tratamiento distinto de la materia por cada una de ellas, con el que las autoridades tratan de remediar los grandes abusos potenciados por los efectos de red de estas grandes empresas tecnológicas.

5. Conclusiones

Tradicionalmente se han considerado los datos desde su vertiente moral o personal, y por tanto como objeto de protección en cuanto derecho fundamental de la persona. Sin embargo, la digitalización de la economía y los mercados, y muy especialmente la entrada en escena de las grandes plataformas digitales, cuyo modelo de negocio reside en parte en la monetización de dichos datos, han puesto de relieve su otra vertiente, la económica o patrimonial. La protección de ambas vertientes, la personal y la económica, está a cargo principalmente de autoridades administrativas –de protección de datos y de competencia, respectivamente–, que necesariamente han de coordinar su análisis y evaluación de conductas de las empresas en el mercado y respecto de los ciudadanos.

En efecto, el *big data* es ya un *input* más en el proceso productivo de las plataformas digitales, y está llamado a ocupar un papel imprescindible en los modelos de negocio de

las empresas que operan en este ecosistema digital, así como en la labor de los Gobiernos y las instituciones públicas en la protección de los bienes que tienen encomendados, desde la propia democracia hasta la salud de los individuos. Aunque los datos no generan *per se* un valor económico por su mera posesión, sí lo hace su procesamiento y tratamiento a través de sistemas de inteligencia artificial, y cuyos resultados pueden interferir en el derecho fundamental de protección de sus datos personales. La necesidad de esta protección ha recibido plasmación normativa, tanto en nuestro texto constitucional y los textos fundacionales de la Unión Europea, como en su regulación en forma de derecho derivado mediante el RGPD.

De esta forma, la sociedad digital y los procesos y sistemas técnicos, que cada vez aparecen con una mayor frecuencia en la forma de nuevas aplicaciones tecnológicas que vienen a facilitar nuestra vida diaria, entrañan toda una serie de riesgos a los que, partiendo de la necesaria protección de la dignidad humana y del libre desarrollo de la personalidad, las autoridades deben atender y responder adecuadamente. Hasta el momento, a pesar de que el RGPD ha colmado algunas de las lagunas que existían en la normativa de protección de datos, como, por ejemplo, a través de la eficacia extraterritorial de sus disposiciones, el legislador comunitario ha olvidado hasta el momento el proceso más peligroso, que debe quedar regulado en el futuro próximo: los sistemas de inteligencia artificial. No en vano el pasado 21 de abril de 2021 la Comisión Europea publicó su propuesta de reglamento sobre la IA.

A pesar de las lagunas –o, en ocasiones, los pronunciamientos contradictorios– que hemos advertido, las autoridades de protección de datos y las autoridades de competencia aún no han encontrado la forma en la que trabajar en paralelo para atajar el procesamiento y tratamiento masivo de los datos personales de los usuarios de la gran mayoría de empresas del mundo, tal vez por las imprecisiones metodológicas de sus análisis o por una falta de herramientas a su disposición para hacerlo. Un primer conato de «entendimiento» conjunto de ambas perspectivas lo encontramos en las dos propuestas de reglamentos aprobadas el pasado 15 de diciembre de 2020, la DSA y la DMA, que aspiran a construir un Mercado Único Digital, respetuoso con los derechos fundamentales y la privacidad de los ciudadanos europeos, a la vez que un eficaz aprovechamiento del potencial económico que la digitalización de las empresas y servicios ofrece.

Con todo y con ello, hemos señalado tres grandes oportunidades que las autoridades de competencia han tenido para tratar de integrar la normativa de protección de datos, aunque sea solapadamente, en sus análisis y valoraciones de las conductas de las empresas, con el fin de proteger el bienestar del consumidor, que también es objetivo último del derecho de la competencia. En primer lugar, la adquisición de Fitbit por parte de Google supuso una sacudida en el ámbito del análisis del control de concentraciones, y la decisión de la Comisión Europea autorizando la operación ha sido muy cuestionada, toda vez que permite al gigante norteamericano la adquisición de ingentes datos de salud de los ciudadanos, con la posible afectación, tanto de su derecho a la protección de sus datos personales como de la competencia en el mercado. En segundo lugar, también hemos examinado en detalle

el periplo de Facebook en sede alemana, en el que la autoridad de competencia construyó su teoría del daño anticompetitivo con base en el incumplimiento del RGPD, por la política de privacidad de la popular red social. Por último, hemos estudiado los embates que en la actualidad afrontan tanto Google como Facebook en los Estados Unidos igualmente por su política de privacidad, así como por la estrategia competitiva que han seguido para eliminar a su competencia actual o potencial en el mercado.

Todo ello nos conduce a afirmar que es necesaria, una vez ya comprobado el valor económico del *big data* en los nuevos modelos de negocio de esta también nueva economía, que se produzcan esas sinergias que proponemos entre autoridades de competencia y autoridades de protección de datos, con tal de evitar decisiones que no estén fundamentadas estrictamente en datos empíricos y que realmente atiendan a las necesidades actuales de protección de los datos personales de los usuarios.

Referencias bibliográficas

Allende Salazar, R. (2020). Capítulo 20. Plataformas digitales y big data: retos para el derecho de la competencia; especial referencia al control de concentraciones. *Anuario de Derecho de la Competencia*, *2020*.

Antón Juárez, I. (2021). Marketplaces que personalizan precios a través del big data y de los algoritmos: ¿esta práctica es legal en atención al derecho de la competencia europeo?, *Cuadernos de Derecho Transnacional*, *13*(1), 44.

Autorité de la Concurrence y Bundeskartellamt. (2016). *Competition Law and Data*.

Buttarelli, G. (2017). Big Data & Competition Law. En *Big Data & Competition Law* (pp. 1-2). Concurrences.

Caffarra, C. y Valetti, T. (4 de marzo de 2020). Google/Fitbit review: Privacy IS a competition issue. *Voxeu Competition Report*. https://voxeu.org/content/googlefitbit-review-privacy-competition-issue

Castillo Parrillas, J. A. (2019). Economía digital y datos entendidos como bienes. En *El mercado digital en la Unión Europea* (pp. 284-288). Reus.

CEPD (Comité Europeo de Protección de Datos). (2014). Privacy and competitiveness in the age of big data.

Davis II, J. S. y Osoba, O. A. (2016). Privacy Preservation in the Age of Big Data: A Survey. Rand Corporation. https://www.rand.org/pubs/working_papers/WR1161.html

Díez Estella, F. (19 de diciembre de 2020). Digital Platforms and Competition Law: the new Digital Markets Act. *EULawLive*. Weekend Edition, *42*, 6-19.

División de Competencia de la OCDE (2016). *Big Data: Bringing Competition Policy to the Digital Era*. https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

Domínguez Álvarez, J. (2021). Privacidad y horizonte tecnológico: algunas reflexiones

al hilo del Pacto Digital impulsado por la Agencia Española de Protección de Datos. *Diario La Ley*, *48*, 4-5.

Ferrer, E. y Pol, A. (2020). Capítulo 5. Protección de datos y derecho de la competencia. En M. A. Recuerda Girela (Dir.), *Anuario de Derecho de la Competencia* (pp. 119-142). Civitas.

Geradin, D. (21 de octubre de 2020). *The U.S. v. Google: A preliminary analysis in ten points*. https://theplatformlaw.blog/2020/10/21/the-u-s-v-*Google*-a-preliminary-analysis-in-ten-points/amp/

Geradin, D. (18 de febrero de 2021). *What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a Digital Market Act?* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3788152.

Gudín Rodríguez Magariños, F. (2018). Parte Específica. Epígrafe 10. Derecho a la protección de datos y las tecnologías disruptivas. En *Nuevo Reglamento Europeo de Protección de Datos vs. Big Data*. Tirant lo Blanch.

Hernández Corchete, J. A. (2018). Capítulo 12. Expectativas de privacidad, tutela de la intimidad y protección de datos. En T. de la Quadra Salcedo y J. L. Piñar Mañas, *Sociedad digital y Derecho* (pp. 293 a 300). Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado.

Herrero Suárez, C. (2018). Capítulo 31. Big Data y Derecho de la Competencia. En T. de la Quadra Salcedo y J. L. Piñar Mañas, *Sociedad digital y Derecho*. Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado.

Ibáñez Colomo, P. (22 de febrero de 2021). The Draft Digital Markets Act: A Legal and Institutional Analysis. https://ssrn.com/abstract=3790276.

International Data Corporation. (2014). The Digital Universe of Opportunities. *International Data Corporation Journal*. https://www.iot-journaal.nl/wp-content/uploads/2017/01/idc-digital-universe-2014.pdf

Krzepicki, A., Wright, J. y Yun, J. (2020). The Impulse to Condemn the Strange: Assesing Big Data in Antitrust. *CPI Antitrust Chronicle*, February 2020, 2-4.

Lambrecht, A. y Tucker, C. E. (2015). Can Big Data Protect a Firm from Competition? https://dx.doi.org/10.2139/ssrn.2705530

Laney, D. (6 de febrero de 2001). 3D Data Management: Controlling Data Volume, Velocity and Variety. *Meta Group* (Gartners Blog post).

Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M. y Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe.

López Galdós, M. (6 de octubre de 2020). The HJC Report on the Future of the U.S. Competition System. https://www.project-disco.org/competition/100620-the-hjc-report-on-the-future-of-the-u-s-competition-system-part-1/.

Martínez López-Sáez, M. (2018). Capítulo 2. La dignidad humana y los derechos personalísimos como punto de partida de un derecho a la protección de datos de carácter personal. En *Una revisión del derecho fundamental a la protección de datos de carácter personal* (pp. 26-27). Tirant lo Blanch.

Martínez, R. (2018). Capítulo 11. Inteligencia artificial, Derecho y derechos fundamentales. En T. de la Quadra Salcedo y J. L. Piñar Mañas, *Sociedad digital y Derecho*. Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado.

Mauro A. de, Greco M. y Grimaldi, M. (2017). *A formal definition of Big Data based in its essential features*. *Library Review*, *65*, 122-

135. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938397.

OCDE (2013). Exploring Data-driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by «Big Data». OECD Publishing. https://www.oecd-ilibrary.org/docserver/5k47zw3fcp43-en.pdf?expires=1616503551&id=id&accname=guest&checksum=F9AA98617C643E05674E3B5E7C487463

Ohlhausen, M. K. y Okuliar, A. P. (2015). Competition, consumer protection, and the right [approach] to privacy, Antitrust Law Journal, Forthcoming, <https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf>.

ONU (Organización de las Naciones Unidas). (2019). Cuestiones de competencia en la economía digital. En *Conferencia de las Naciones Unidas sobre Comercio y Desarrollo* (p. 2). https://unctad.org/system/files/official-document/ciclpd54_es.pdf

Petit, N. y Teece, D. (2021). Big Tech, Big Data, And Competition Policy: Favouring Dynamic Over Static Competition. SSRN. https://ssrn.com/abstract=3229180

Petit, N., Teece, D. J. y Berkeley Research Group Institute. (2021). Big tech, Big Data, and Competition policy: favoring dynamic over static competition (pp. 29-31). https://dx.doi.org/10.2139/ssrn.3229180

Piñar Mañas, J. L. (2018). Capítulo 3. Identidad y persona en la sociedad digital. En T. de la Quadra Salcedo y J. L. Piñar Mañas, *Sociedad digital y Derecho*. Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado.

Quadra-Salcedo Fernández del Castillo, T. de la. (2018). Capítulo 1. Retos, riesgos y oportunidades de la sociedad digital. En T. de la Quadra-Salcedo Fernández del Castillo y J. L. Piñar Mañas, *Sociedad digital y Derecho*. Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado.

Sokol, D. D. y Comerford, R. (2016). Antitrust and Regulating Big Data. *George Mason Law Review, 23(119)*, 1.133-1140. University of Florida Levin College of Law Research. https://ssrn.com/abstract=2834611.

Troncoso Reigada, A. (2010). Capítulo primero. La configuración constitucional de un derecho fundamental a la protección de datos personales y su desarrollo por el legislador. En *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Volmara, N. M. y Helmdachb O. K. (2018). Protecting consumer and their data trough competition law? Rethinking abuse of dominance in light of Federal Cartel Office's Facebook investigation. *European Competition Journal*, *14*(2-3), 195-215. https://doi.org/10.1080/17441056.2018.1538033.

Waler, K. (20 de octubre de 2020). A deeply flawed lawsuit that would do nothing to help consumers. https://blog-*Google*.cdn.ampproject.org/c/s/blog.*Google*/outreach-initiatives/public-policy/response-doj/amp/