DERECHO DE LA COMPETENCIA VS. PRIVACIDAD: ¿EL GRAN DILEMA EN LOS NUEVOS MERCADOS DIGITALES?

ANTITRUST VS. PRIVACY: THE GREAT DILEMMA IN THE NEW DIGITAL MARKETS?

Fernando Díez Estella
Profesor Titular acreditado de Derecho Mercantil
Universidad Villanueva
ORCID ID: 0000-0002-5011-0051

Alba Ribera Martínez
Doctoranda en Derecho de la Competencia
Universidad Carlos III de Madrid
ORCID ID: 0000-0002-9152-0030

Recibido: 27.12.2021 / Aceptado: 12.01.2022
DOI: https://doi.org/10.20318/cdt.2022.6682

Resumen: La digitalización de los modelos empresariales existentes y la nueva forma de hacer negocios de las plataformas digitales plantean nuevos retos tanto en la actuación de las empresas en el mercado como en la vida de los consumidores y usuarios. Las empresas digitales dominantes son todas estadounidenses (Google, Facebook, Amazon y Apple), y sus prácticas parece que lesionan la libre competencia en los mercados. Este fenómeno plantea el reto de cómo afrontar la regulación del Big Data, al que hasta ahora no se ha dado una respuesta del todo satisfactoria. En este trabajo se analiza también el contenido constitucional de la privacidad y su importancia en el marco de los análisis de competencia realizados a ambos lados del Atlántico.
Palabras clave: Big Data, privacidad, mercados digitales, antitrust.

Abstract: The digitisation of existing business models and the new way of doing business of digital platforms pose new challenges both to the performance of companies in the market and to the lives of consumers and users. The dominant digital companies are all American (Google, Facebook, Amazon, and Apple), and their practices appear to harm free competition in the markets. This phenomenon raises the challenge of how to deal with the regulation of Big Data, to which so far there has not been an entirely satisfactory response. This paper also analyses the constitutional content of privacy and its importance in the framework of competition analyses carried out on both sides of the Atlantic.
Keywords: Big Data, privacy, digital markets, antitrust.

B) Suspensión de la decisión en primera instancia. C) Pronunciamiento sobre la decisión en segunda instancia. 3. La perspectiva estadounidense. A) El DOJ (y otros estados) c. Google. B) La FTC c. Facebook: un viaje de ida y vuelta. V. Conclusiones.

I. Introducción

1. En el pasado mes de marzo de 2021 el Parlamento Europeo emitió su informe sobre la Estrategia Europea de Datos[1][2], en el que se señala que los datos se han convertido en un nuevo activo económico, que ya es un requisito para asegurar la viabilidad y competitividad de las empresas. A partir de esta premisa, este informe señala la necesidad de una regulación en esta materia, con el fin de conformar a nivel comunitario una sociedad de los datos, acorde con los derechos y valores de la Unión Europea (UE).

2. Más adelante, el informe 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[3] 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*).

3. Este cambio ha planteado la exigencia de que la Administración Pública, en alguna de sus formas, intervenga en estos mercados, siendo posible dicha intervención regulatoria tanto a nivel nacional como en sede de organismos comunitarios e internacionales. Frente a este reto, caben dos posibles líneas de actuación: por una parte, la regulación económica *ex ante* de los mercados y, por otra, los instrumentos *ex post* propios de la normativa de Derecho de la Competencia, ambos como límite a la libertad de empresa de los operadores de estas plataformas digitales. Todo ello desde la duda, todavía no resuelta (ha sido acertadamente caracterizada como el *antitrust privacy dilemma*[4]), de hasta qué punto las consideraciones sobre privacidad han de integrarse en el Derecho de la competencia[5]; el efecto de las normas de protección de datos sobre la competencia; y, las teorías del daño basadas en la protección de la privacidad[6].

4. 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 UE en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (en adelante CDFUE), y en el ámbito nacional en el art. 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.

5. Por lo que se refiere a la regulación de materias relacionadas con estas plataformas digitales, en el ámbito de la Unión Europea se ha visto reflejada en la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas

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

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data (COM/2020/66 final).

[3] Naciones Unidas, Cuestiones de competencia en la economía digital, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 2009, disponible en: https://unctad.org/system/files/official-document/ciclpd54_es.pdf.

[4] C. Carugati, "The Antitrust Privacy Dilemma", *SSRN*, noviembre de 2021, disponible en: https://ssrn.com/abstract=3968829.

[5] F. Costa-Cabral. y O. Lynskey, "Family ties: the intersection between data protection and competition in EU Law", *Common Market Law Review*, 54 (1), 2017, pp. 11-50.

[6] M. Botta y K. Wiedemann, "The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*", The Antitrust Bulletin*, Vol. 64(3), 2019, pp. 428-446.

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) [7].

6. En España, la transposición del RGPD provocó un proceso de "actualización" de la normativa en materia de protección de los datos personales, que culminó con la promulgación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD en adelante) [8]. El pasado mes de julio de 2021 se ha vuelto a dar un paso más en esta materia con la aprobación de una Carta de Derechos Digitales a nivel nacional[9].

7. En paralelo a estos avances que se están produciendo en sede de protección de datos, 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 propias autoridades de protección de datos, que expondremos a continuación.

8. 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/usuarios, que posteriormente se monetizan a partir de su uso con fines publicitarios.

9. En este trabajo vamos a explorar cuál es la regulación existente del *Big Data* en relación con la protección del derecho a la protección de datos personales, cuya protección radica de su protección en el rango constitucional a partir de la propia Constitución Española y de la Carta de Derechos Fundamentales de la Unión Europea. Paralelamente, también abordaremos los aspectos relativos a la privacidad, que es un concepto más amplio y no tan apegado exclusivamente a la persona, en relación con los pasos que se están dando en el ámbito de su regulación[10].

10. También expondremos las posibilidades que el Derecho de la Competencia ofrece, que tienden 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 *Google/Facebook* tanto a un lado del Atlántico como al otro.

11. A estos efectos, analizaremos si el análisis *antitrust*, encargado de velar por el mantenimiento de un mercado competitivo y de proteger a los consumidores, es suficientemente versátil para adaptarse a estas nuevas realidades, o si debe actualizarse. Ante las insuficiencias que el Derecho de la Competencia ha presentado hasta ahora, tras varios años de trabajos preparatorios, consultas y documentos de trabajo, el 15 de diciembre de 2020 la Comisión Europea presentó dos propuestas de Reglamentos - la *Digital Markets Act*[11] (en adelante DMA) y la *Digital Services Act*[12] (en adelante DSA)- que pretenden reconfigurar la realidad de los servicios y mercados digitales[13] en la UE de los próximos años.

---

[7] 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 (Reglamento general de protección de datos) *DOUE* L 119, 4.5.2016, p. 1–88.

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *BOE* de 6 de diciembre de 2018.

[9] Disponible en la web del Ministerio de Asuntos Económicos y Transformación Digital: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210714_np_Carta-.aspx.

[10] Competition & Markets Authority y Information Commissioner's Office., *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 de mayo de 2021, pp. 1-31.

[11] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales), Bruselas, 15 de diciembre de 2020, COM (2020) 842 final.

[12] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se notifica la Directiva 2000/31/CE, Bruselas, 15 de diciembre de 2020, COM (2020) 825 final.

[13] F. Díez Estella, *"*Digital Platforms and Competition Law: the new Digital Markets Act*"*, *EULawLive*, Weekend Edition

Por ahora, la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo ya ha emitido su informe sobre ambas propuestas[14]. Mientras que el Parlamento Europeo ya ha dado luz verde al Consejo para comenzar las negociaciones con los Estados miembros respecto de la propuesta de DMA, la propuesta de DSA solamente ha superado el trámite de la Comisión de Mercado Interior[15].

12. Esta propuesta, no exenta de polémica[16], 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*»[17] (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.

13. Tanto la DMA como la DSA forman parte del *Digital Services Act package*, que es uno de los ejes de la Estrategia Digital Europea. Esta estrategia, presentada oficialmente en febrero de 2020, tiene como objetivo conformar «*una sociedad europea impulsada por soluciones digitales que sitúan en el 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*»[18]. Para ello se presentan dos documentos básicos: la Estrategia Europea de Datos mencionada anteriormente y las opciones estratégicas destinadas a garantizar un desarrollo de la inteligencia artificial centrado en el ser humano[19], que se va a incorporar a la regulación a nivel comunitario a través de la propuesta de Reglamento de Inteligencia Artificial presentada por la Comisión Europea el pasado 21 de abril de 2021[20].

14. 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 sólo 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.

15. 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. También realizaremos un breve comentario a los casos *Google* y *Facebook* que se están desarrollando al otro lado del Atlántico, a raíz del nuevo impulso que el Derecho

---

nº42, diciembre 2020, pp. 6-19; P. Ibañez Colomo, "The Draft Digital Markets Act: A Legal and Institutional Analysis", *Journal of European Competition Law & Practice*, 12, febrero 2021, pp. 561-575

[14] Committee on the Internal Market and Consumer Protection, *Report on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, COM (2020) 0842; European Parliament- Press Release: "Digital Services Act: a safer online space for users, stricter rules for platforms", 14 de diciembre de 2021.

[15] European Parliament – Press Release: "Digital Markets Act: Parliament ready to start negotiations with Council", 15 de diciembre de 2021.

[16] Es particularmente acertado el análisis crítico que lleva a cabo, en fechas muy recientes: akman, p., "Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act", *European Law Review* (forthcoming, 2020).

[17] D. Geradin, "What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a Digital Market Act?", *SSRN*, febrero 2021, disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3788152.

[18] Comisión Europea - Comunicado de prensa: "Dar forma al futuro digital de Europa: la Comisión presenta sus estrategias en relación con los datos y la inteligencia artificial", Bruselas, 19 de febrero de 2020, IP/20/273.

[19] Comisión Europea, *Libro Blanco sobre la inteligencia artificial – un enfoque orientado a la excelencia y la confianza*, Bruselas, 19 de febrero de 2020, COM (2020) 65 final,

[20] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, Bruselas, 21 de abril de 2021, COM (2021) 206 final.

de la Competencia ha adquirido sobre todo en EE. UU en el último año, a partir de la Orden Ejecutiva emitida por el presidente Biden el 9 de julio de 2021[21].

16. 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 II). 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 III). Así mismo, 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 IV). Finalmente, se ofrece un apartado de conclusiones (epígrafe V).

II. Explotación del Big Data vs. derecho a la Privacidad

1. Caracterización del Big Data

17. Las autoridades de competencia y las autoridades de protección de datos han detectado las sinergias existentes entre el interés en proteger los datos de los consumidores -especialmente personales- y de la tensión competitiva en los mercados como consecuencia de la generación del *Big Data* a nivel global[22].

18. Tal y como expusieron las autoridades alemana y francesa en 2016, el fenómeno del *Big Data* semánticamente procede de la importancia de los datos no solo en las plataformas digitales sino también en todas aquellas empresas presentes en el sector digital (la mayoría), e incluso en la toma de decisiones de los Gobiernos[23]. No obstante, es verdad que son las plataformas puramente digitales las que han centrado su modelo de negocio sobre la base de la captación y utilización intensiva de datos[24].

19. El *Big Data* está compuesto por flujos de información procedentes de una gran cantidad de fuentes de datos, que van desde los datos personales producidos por los usuarios en línea, directa o indirectamente, hasta aquellos que conciernen los aspectos del mundo real, como por ejemplo la geolocalización del usuario en el mundo físico. 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*»[25].

20. Esta definición se basa en el modelo de las «3V» teorizado por Douglas Lanely que describe las principales características del *Big Data: Volumen, Velocidad* y *Variedad*[26]*,* acogida por gran parte

[21] Presidental Actions (Joseph R. Biden JR.) – Briefing Room: "Executive Order on Promoting Competition in the American Economy", Washington, 9 de julio de 2021.

[22] Competition & Markets Authority y Information Commissioner's Office., *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 de mayo de 2021, pp. 1-31. (p. 3).

[23] Autorité de la Concurrence y Bundeskartellamt, *Competition Law and Data*, 10 de mayo de 2016, pp. 1-54 (pp. 4-5); I. Antón Juárez, "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), 2021, pp. 42-69 (p. 44).

[24] R. Allendesalazar, "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, noviembre de 2020, pp. 1-38 (p. 6).

[25] Directorate for Financial and Enterprise Affairs (Competition Committee), *Big Data: bringing competition policy into the digital era*, 27 de octubre de 2016, DAF/COMP(2016)14. La OCDE retoma la definición adoptada en A. De Mauro, M. Greco, M. Grimaldi*,* "A formal definition of Big Data based in its essential features", *Library Review*, Vol. 65 (3), marzo 2017, pp. 122-135.

[26] D. Laney, "3D Data Management: Controlling Data Volume, Velocity and Variety", Meta Group (Gartners Blog post), febrero 2001.

de la doctrina[27]. Por tanto, 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 tradicionalmente se han venido procesando estos mismos datos mediante estudios de mercado y muestreos con una finalidad meramente publicitaria[28]. 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.

21. La característica más importante y también más discutida, 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. 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. Desde la perspectiva puramente económica, la obtención indiscriminada de datos personales no supone un valor añadido *per se* a la empresa[29]. Algunos autores, tomando la comparación con el proceso productivo, designan a estos datos como el *raw data*[30].

22. Así, Lambrecht Y Tucker 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*» [31]. Según sostienen, existen escasas barreras a la entrada en el mercado de los datos. Los datos almacenados por una empresa son replicables y pueden perder su valor rápidamente. En cambio, aquellos datos que son especialmente valiosos son los datos agregados y actualizados[32].

23. En sentido ligeramente opuesto, otros autores sostienen que el *Big Data,* especialmente aquel que contiene tendencias de consumo, es susceptible de ser reutilizado a un coste marginal reducido, y como tal se trata de un activo no despreciable. En los mercados puramente digitales prevalece el enfoque de capacidades, es decir, las empresas que lo componen deben adaptarse constantemente a los cambios que se producen en él (por ejemplo, frente a la entrada de un nuevo competidor en el mercado)[33].

24. Por tanto, las barreras de entrada y acceso a este tipo de mercados digitales no se identifican tanto por su falta de replicabilidad sino la escala a la que se utilizan. Como es lógico, le resultará más fácil replicar los datos de sus competidores e incluso conformar sus propias bases de datos a aquellas empresas con mayores economías de escala y alcance y, con una mayor capacidad de inversión inicial frente a los nuevos entrantes que se verán obligados a invertir en lo que, en principio, serán costes hundidos en datos[34].

---

[27] OCDE, "Exploring Data-driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", *OECD Digital Economy Papers*, No. 222, junio 2013, pp. 1-44 (pp. 11-12).

[28] I. Antón Juárez, "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), 2021, pp. 42-69 (pp. 52-53).

[29] D.D. Sokol y R. Comerford, "Antitrust and Regulating Big Data", *George Mason Law Review*, 119 (23), septiembre 2016, pp. 1129-1161 (pp. 1135-1140).

[30] J.A. Castillo Parrillas, "Economía digital y datos entendidos como bienes", en I.L. Martens Jiménez y A. M. Pastor García (Coord.), *El mercado digital en la Unión Europea*, Madrid, Reus Editorial, 2019, pp. 279-301 (pp. 284-288).

[31] A. Lambrecht Y C.E. Tucker, "Can Big Data protect a firm from competition?", *SSRN*, diciembre 2015, disponible en: https://ssrn.com/abstract=2705530.

[32] D.D. Sokol y R. Comerford, "Antitrust and Regulating Big Data", *George Mason Law Review*, 119 (23), septiembre 2016, pp. 1129-1161 (pp. 1135-1140).

[33] N. Petit Y D.J. Teece, "Innovating Big Tech Firms and Competition Policy: Favoring Dynamic Over Static Competition", *Industrial and Corporate Change*, marzo 2021, pp. 1-31 (pp. 20-31).

[34] Competition & Markets Authority y Information Commissioner's Office., *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 de mayo de 2021, pp. 1-31. (p. 11-12); M. Gal Y O. Aviv, "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*, forthcoming 2020, pp.1-37 (pp. 7-11)..

25. Sin perjuicio de estas discusiones doctrinales, estos datos resultan valiosos por cuanto pueden ser utilizados eficiente y rápidamente para refinar y predecir el comportamiento humano con fines comerciales a partir de las interacciones de los usuarios en línea[35]. De esta forma, son susceptibles de ser tratados como un *input* más en el proceso productivo, por ejemplo, para acelerar los procesos de I+d dentro de la empresa[36].

26. Los datos a los que aludimos no solo son los datos personales facilitados de forma voluntaria y consciente por el usuario, como lo es por ejemplo su fecha de nacimiento o sexo cuando se registrar en una plataforma digital[37]. Las empresas también almacenan aquellos datos que proceden de la "huella digital" que el usuario genera en la propia plataforma (por ejemplo, a través de sus *likes* en Instagram) o en páginas terceras no necesariamente relacionadas con la plataforma digital concreta[38]. Por tanto, el *Big Data* también está integrado por datos no personales, seudonimizados o anonimizados[39].

27. 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[40]), mientras que en 2009 esta cifra solamente era de 5 ZB[41].

28. Todos estos datos, recopilados y puestos en común, permiten que los sistemas de inteligencia artificial reproduzcan el comportamiento humano de forma automatizada (en adelante IA). Estos sistemas de IA tienen distintas variantes, de forma que algunos pueden deducir patrones y tendencias de consumo a partir de los datos que los alimentan (*machine learning)* mientras que otros podrán razonar y sacar sus propias conclusiones imitando la capacidad de raciocinio humana (*deep learning)*.

29. 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 optimización de los sistemas de IA[42]. Buena muestra de ello es el paso hacia adelante que ha tomado *Meta* (antiguo *Facebook*) a través de la presentación de su proyecto de metaverso[43]. Las plataformas digitales han traído consigo, por tanto, la posibilidad de que los operadores en el mercado obtengan una ventaja competitiva en el mercado incorporando el *Big Data* en su propia actividad o incluso permitiéndoles que los puedan vender a terceros (*brókers)*[44].

---

[35] A. Krzepicki, J. Wright y J. Yun, "The Impulse to Condemn the Strange: Assessing Big Data in Antitrust", *CPI Antitrust Chronicle*, 2(2) febrero 2020, pp. 16-20 (pp. 18-20); Directorate for Financial and Enterprise Affairs (Competition Committee), *Big Data: bringing competition policy into the digital era*, 27 de octubre de 2016, DAF/COMP(2016)14 (pp. 7-8).

[36] Directorate for Financial and Enterprise Affairs (Competition Committee), *Big Data: bringing competition policy into the digital era*, 27 de octubre de 2016, DAF/COMP(2016)14 (pp. 7-15); OCDE, "Exploring Data-driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", *OECD Digital Economy Papers*, No. 222, junio 2013, pp. 1-44 (pp. 12-13); D.D. Sokol y R. Comerford, "Antitrust and Regulating Big Data", *George Mason Law Review*, 119 (23), septiembre 2016, pp. 1129-1161 (pp. 1133-1140);

[37] T. De La Quadra-Salcedo Fernández Del Castillo, *"Cap. 1. Retos, riesgos y oportunidades de la sociedad digital"*, en T. De La Quadra Salcedo Y J.L. Piñar Mañas, *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 21- 87 (pp. 35 y 36).

[38] I. Antón Juárez, "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), 2021, pp. 42-69 (p. 42); Competition & Markets Authority y Information Commissioner's Office., *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 de mayo de 2021, pp. 1-31 (p. 11).

[39] European data protection supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, marzo 2014, pp. 1-41 (p. 9).

[40] Este concepto denota una unidad de almacenamiento de información que equivale a 10^{21} bytes.

[41] International Data Corporation, "The Digital Universe of Opportunities", *Needham: International Data Corporation Journal,* abril 2014, pp. 1-17 (p. 3).

[42] R. Allendesalazar, "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, noviembre de 2020, pp. 1-38 (p. 11-15).

[43] Meta- Newsroom: "Introducing Meta: A Social Technology Company", octubre de 2021.

[44] I. Antón Juárez, "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), 2021, pp. 42-69 (p. 44).

30. Frente a esta descripción, aquello que está preocupando más a autoridades de competencia y de protección de datos sobre el *Big Data* precisamente es su contenido. Hoy en día, un estudio ya demuestra que es posible identificar al 87% de la población de EE. UU a partir de su código postal, fecha de nacimiento y sexo, datos que nos podrían parecer a primera vista como "inofensivos" [45]. 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 con estos mismos fines (lo que se conoce en el sector del marketing como *profiling*[46]).

31. De esta forma, los operadores pueden dirigirse fácilmente a sus usuarios porque pueden inferir sus hábitos de consumo y preferencias a partir de los datos obtenidos de otros usuarios con perfiles de consumo similares. Así, se pueden producir decisiones de negocio en el *scoring* bancario o en el análisis de riesgos que se realiza para la contratación de un seguro con base en datos que ni siquiera se han aportado por el propio usuario[47]. Además, nos podemos encontrar con la situación en la que estas mismas herramientas induzcan artificialmente al consumo de determinados productos al usuario según la identidad y perfil definidos que se han cotejado a partir de sus interacciones en línea[48].

32. Por el propio funcionamiento de "caja negra"[49] 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 estos 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 (aunque no deberían) utilizarlos para fines completamente distintos a aquellos que motivaron su transferencia en primer lugar[50].

2. Gratuidad para el usuario, ingente beneficio para la plataforma

33. Los usuarios de las grandes plataformas digitales disfrutan de sus servicios gratuitamente[51]. 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*).

34. 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 eficiente-

[45] J.S. Davis Ii, Y O.A. Osoba, "Privacy Preservation in the Age of Big Data*" RAND Corporation*, enero 2016, disponible en https://www.rand.org/pubs/working_papers/WR1161.html.

[46] European data protection supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, marzo 2014, pp. 1-41 (p. 10).

[47] R. Martínez Martínez, "Cap. 11. Inteligencia artificial, Derecho y derechos fundamentales", en T. De La Quadra Salcedo Y J.L. Piñar Mañas (Coord.), *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 259-279 (pp. 264 a 267).

[48] J.L. Piñar Mañas, "Capítulo 3. Identidad y persona en la sociedad digital", en T. De La Quadra Salcedo Y J.L. Piñar Mañas, *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 95-113 (pp. 101 a 103).

[49] R. Martínez Martínez, "Cap. 11. Inteligencia artificial, Derecho y derechos fundamentales", en T. De La Quadra Salcedo Y J.L. Piñar Mañas (Coord.), *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 259-279 (pp. 262 a 264).

[50] European data protection supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, marzo 2014, pp. 1-41 (p. 9).

[51] Naturalmente, esta gratuidad no es tal, sólo aparente, y por ello pagan un elevado precio, no monetario, pero sí en términos de sus datos personales; *Vid.*, sobre esta cuestión: H. Jenkins, D. Jevons, Y A. Mell, "Competing For Free", *CPI Antitrust Chronicle*, September 2021, 2021, pp. 1-8 (pp. 2 a 7); M. Gal Y D.L. Rubinfeld, "The Hidden Costs of Free Goods: Implications for Antitrust Enforcement", *NYU Center for Law, Economics and Organization,* Law & Economics Research Paper Series Working Paper nº 14-44, enero 2015, pp. 1-59.

mente, producirán unos resultados más relevantes, focalizados y pertinentes[52] para predecir las tendencias de consumo que se pueden dar en relación con los servicios prestados por la plataforma (*feedback loop)*. Estos efectos de red tradicionalmente generan un interés en los dos lados de la plataforma; esta ofrece el espacio de su plataforma a los anunciantes, de forma que sus usuarios acceden gratuitamente a sus servicios porque están 'subvencionados' por las compras que se realizan en el otro lado del mercado.

35. 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, tal y como aparentemente pudiera parecer[53]. Normalmente, el usuario cae en este equívoco influido por la sensación de gratuidad del servicio 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 y no personales. En virtud de ello, la plataforma digital recibe un influjo constante de *Big Data* con un elevado valor comercial[54].

36. 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 estos mismos datos[55].

3. Enfoque desde la perspectiva de los derechos fundamentales

37. Hemos indicado anteriormente que el *Big Data* no solamente contiene datos personales, sino que también puede contar datos no personales. Dentro de esta misma concepción se mueve la consideración de la privacidad del individuo, en cuya esfera más amplia encontramos el derecho a la protección de datos personales. El derecho a la protección de datos personales protege el tratamiento de aquella información sobre una persona física que permita identificarla. Se dispensa protección a todos aquellos datos que permitan la identificación de la persona, y no solamente a aquellos datos más íntimos. Este y solo este es el objeto de protección del RGPD, *ex* artículo 4. El derecho fundamental a la protección de datos personales protege a este conjunto de información que, de forma contraria al principio de igualdad pueda ser utilizada para justificar decisiones públicas o privadas. 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*»[56].

38. Por una parte, el art. 8 CDFUE protege en concreto este derecho, cuyo tratamiento se sujeta a una serie de principios, concretizándose en un gran poder de intervención institucional sobre las modalidades de su tratamiento[57]. Haciendo uso de la competencia específica que se le confiere en el TFUE, el Tribunal de Justicia de la Unión Europea ha ido delimitando el alcance del procesamiento de los datos personales de los usuarios en línea mediante sucesivos pronunciamientos, aun antes del hito que supuso la aprobación y aplicación del RGPD, al que nos referiremos posteriormente.

---

[52] C. Herrero Suárez, "Cap. 31. Big Data y Derecho de la Competencia*"*, en T. De La Quadra Salcedo, Y J.L. Piñar Mañas, *Sociedad digital y Derecho,* Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 659-683 (pp. 666 a 672).

[53] R. Allendesalazar, "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, noviembre de 2020, pp. 1-38 (pp. 4-5).

[54] European data protection supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, marzo 2014, pp. 1-41 (pp. 10-32).

[55] J.A. Hernández Corchete, "Cap. 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,* Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 279-301 (pp. 293 a 300).

[56] J.L. Piñar Mañas, "Capítulo 3. Identidad y persona en la sociedad digital", en T. De La Quadra Salcedo Y J.L. Piñar Mañas, *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 95-113 (pp. 109 a 111).

[57] M. Martínez López-Saez, "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 M. Martínez López Sáez, *Una revisión del derecho fundamental a la protección de datos de carácter personal*, Valencia, Tirant lo Blanch, 2018, pp. 43-61 (p. 43-44).

39. En 2016 en el Asunto *Digital Rights Ireland Ltd*, 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[58]. Por tanto, las garantías que tienden a la protección del individuo en este sentido son especialmente relevantes en aquellos casos que los datos personales se someten a un tratamiento automático.

40. De forma similar, la Gran Sala del Tribunal Europeo de Derechos Humanos (TEDH) determinó que para ponderar si efectivamente se ha producido una violación del derecho al respeto de la vida privada y familiar, se debe atender al tratamiento de esos datos personales, tanto respecto de los procesos a los que se iba a someter como a los resultados que se fueran a obtener[59].

41. Por otra parte, a nivel nacional, el derecho a la protección de datos personales se deriva del contenido del artículo 18 CE, de forma autónoma al derecho a la intimidad[60]. Con idéntico sentido que en la jurisprudencia comunitaria se ha identificado que ambos derechos comparten un fundamento común: la dignidad humana cuyo respeto se reconoce en el art. 10.1 CE[61].

42. El tratamiento de los datos personales supone un riesgo para el individuo en cuanto a la construcción digital que se puede realizar de él a partir de sus datos[62]. Por ello, desde una perspectiva regulatoria se trata de reconducir el control de estos datos personales mediante determinadas salvaguardas en favor de su titular.

43. El contorno y los límites de este derecho a la protección de datos personales es objeto de un intenso debate puesto que las manifestaciones tecnológicas y técnicas que suponen una amenaza a este control en manos del usuario se lanzan cada vez con más rapidez. La jurisprudencia europea ya ha lidiado con algunas de estas manifestaciones. Por ejemplo, en el caso de la videovigilancia se ha circunscrito la posibilidad del almacenamiento y tratamiento de las grabaciones de imágenes a un mínimo, aun cuando los motivos que las justifiquen sean especialmente loables[63].

44. Sin embargo, en la mayoría de los casos la tecnología va un paso por delante del legislador y poder judicial comunitario y nacional, en la medida que se producen lanzamientos constantes en el mercado de nuevas aplicaciones y sistemas tecnológicos[64]. El sector del Internet de las cosas (IoT), compuesto por productos tales como los asistentes virtuales -*Siri, Alexa y Google Assistant*-, es un buen ejemplo de ello. Este nuevo fenómeno digital se caracteriza por su desregulación, a pesar de los riesgos que entraña respecto al tratamiento de datos personales y no personales. En este sentido, desde la Comisión Europea ya se ha advertido de la existencia de este 'vacío regulatorio' y en noviembre de 2021

[58] STJUE 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 51 a 55.

[59] SSTEDH de 4 de diciembre de 2008, *S. y Marper c/ Reino Unido*, 30562/04 y 30566/04, apartado 67; 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.

[60] STC 30 de noviembre de 2000 (*RTC* 2000/292).

[61] STS de 28 de febrero de 2008 (*RJ* 2008/2932).

[62] M. Martínez López-Saez, "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 M. Martínez López Sáez, *Una revisión del derecho fundamental a la protección de datos de carácter personal*, Valencia, Tirant lo Blanch, 2018, pp. 43-61 (pp. 43-46).

[63] STJUE 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; STEDH de 2 de septiembre de 2010, *Uzun c. Alemania*, 35623/05 ECLI: CE: ECHR:2010:0902JUD003562305, apartado 46.

[64] T. De La Quadra-Salcedo Fernández Del Castillo, *"Cap. 1. Retos, riesgos y oportunidades de la sociedad digital"*, en T. De La Quadra Salcedo Y J.L. Piñar Mañas, *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 21- 87 (pp. 45-51); F. Gudín Rodríguez Magariños, "Parte Especial. Epígrafe 10. Derecho a la protección de datos y las tecnologías disruptivas", en F. Gudín Rodríguez Magariños, *Nuevo Reglamento Europeo de Protección de Datos vs. Big Data*, Valencia, Tirant lo Blanch, 2018, pp. 297-318.

ya lanzó un informe preliminar sobre los posibles peligros generados por estas tecnologías con el fin de darle una respuesta desde la perspectiva de la política de competencia[65]. Sin embargo, hasta ahora no se han definido los límites y garantías que deben regir en su ejercicio para asegurar la pervivencia del control de los datos personales en su titular.

45. En este mismo sentido, nos encontramos 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[66]. Hasta el momento, solamente se ha regulado de forma general a través de las disposiciones del RGPD[67].

46. Esta manifestación tecnológica es especialmente acuciante en cuanto a sus riesgos, puesto que en la actualidad este servicio lo proveen casi en exclusiva las grandes plataformas digitales americanas, de forma que existe una absoluta dependencia de estos proveedores internacionales para la provisión del servicio. En el marco de la Estrategia de Datos Europea, con el fin de preservar la soberanía de datos europea, actualmente se está trabajando en el proyecto *Gaia-X*, es decir, la nueva plataforma Cloud federada Europea.

47. Estos fenómenos tecnológicos entrañan riesgos para la protección de los datos personales de los usuarios y es prácticamente inútil que el legislador trate, en sede de regulación, de atajar aisladamente cada manifestación tecnológica[68]. Hasta el momento, las propuestas de DMA y DSA que tenemos sobre la mesa tratan de realizar precisamente esto, de forma aislada al Derecho de la Competencia, pero también respecto del ámbito de la protección de datos.

III. Regulación e intervención administrativa en los mercados digitales

1. La protección de los datos a partir del RGPD

48. Sobre la base jurídica del art. 8 CDFUE y en relación con el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) desde el 25 de mayo de 2018 es de aplicación obligatoria en el conjunto de Estados miembros de la Unión el RGPD[69]. Esta es la regulación de la que se ha dotado a las personas físicas este lado del Atlántico para la protección del tratamiento de los datos de carácter personal de acuerdo con las exigencias del siglo XXI[70].

49. Frente a la amenaza que suponen las *GAFA*, residenciadas en su mayoría en EE. UU, y que, hasta hace poco escapaban del alcance del regulador comunitario, el RGPD dota de eficacia extraterritorial a sus disposiciones[71]. De esta forma, como ya había sostenido la jurisprudencia comunitaria, le

---

[65] Press Statement – European Commission: "Questions & Answers – Antitrust: Commission publishes preliminary report on consumer Internet of Things sector inquiry", Bruselas, 9 de junio de 2021, QANDA/21/2908.

[66] Grupo de Protección de Datos del Artículo 29, *Dictamen 05/2012 sobre la computación en nube,* 1 de julio de 2012, 01037/12/ES.

[67] Agencia Española de la Protección de Datos, *Guía para clientes que contraten servicios de Cloud Computing*.

[68] J.A. Hernández Corchete, "Cap. 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,* Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 279-301 (pp. 279-295).

[69] Versión consolidada del Tratado de Funcionamiento de la Unión Europea, *OJ* C 326, 26 de octubre de 2012, p. 47–390.

[70] Desde 1995 ya existía una regulación a nivel comunitario tendente a armonizar la protección de los derechos y libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de carácter personal, a través de la Directiva 95/46/CE.

[71] J.A. Hernández Corchete, "Cap. 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,* Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 279-301 (pp. 288 a 290).

son aplicables las salvaguardas del RGPD a aquel tratamiento de datos que se desarrolla fuera de las fronteras comunitarias[72].

50. En este sentido, el RGPD en su art. 3 garantiza que se produzca este flujo transfronterizo de la regulación, ya que se aplica el principio de territorialidad de aplicación de las normas, que sitúa el centro de gravedad de la relación jurídica en la nacionalidad del titular de los datos personales. 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 a la nacionalidad del titular de los datos personales.

51. El RGPD impone al responsable del tratamiento de esos datos personales toda una serie de exigencias regulatorias con el fin de proteger al consumidor/usuario, y lo hace de acuerdo con el principio de responsabilidad proactiva, ex artículo 5.2 RGPD[73]. Es decir, le corresponde a este demostrar y acreditar el cumplimiento de los principios instituidos por el RGPD.

52. En primer lugar, debe regir en su actuación tanto el principio de minimización de datos -es decir, que solamente se utilicen datos adecuados, pertinentes y necesarios para los fines a los que se van a destinar-, como de anonimización (cuando sea posible) en el acceso a los datos personales de sus usuarios[74]. El tratamiento de datos se debe regir por el principio de licitud. Es decir, debe haber una causa suficiente que motive que el encargado del tratamiento almacene y procese los datos personales de personas físicas.

53. Como cabría suponer, uno de los principales motivos que pueden sustentar la licitud del tratamiento es el consentimiento de la persona que será individualizada mediante el acceso a estos datos, *ex* 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.

54. En caso de que no concurra esta circunstancia, el RGPD prevé otros supuestos en que el tratamiento de datos personales será también lícito. Una de las causas más discutidas precisamente por su relación con el *Big Data* es aquella del art. 6.1.b) RGPD: la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

55. El CEPD ha analizado en particular este motivo de licitud del tratamiento, por cuanto que en esta causa se suele fundamentar el almacenamiento y procesamiento de grandes grupos de datos con el fin de las tareas de *profiling* que señalábamos anteriormente en el mercado adyacente de la publicidad en línea. En este sentido, en sus Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados señala que el responsable del tratamiento de datos personales no puede ampliar artificialmente los tipos de operaciones a las que se someten de forma indiscriminada[75]. Sin embargo, en la

[72] STJUE 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.

[73] J.A. Hernández Corchete, "Cap. 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,* Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 279-301 (pp. 283 a 290).

[74] R. Martínez Martínez, "Cap. 11. Inteligencia artificial, Derecho y derechos fundamentales", en T. De La Quadra Salcedo Y J.L. Piñar Mañas (Coord.), *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 259-279 (pp. 275 a 277).

[75] European data protection board, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 de octubre de 2019.

práctica, observamos como este el principal talón de Aquiles de la regulación, que sigue amparando que las grandes plataformas digitales almacenen y procesen grandes cantidades de datos a una gran velocidad, generando un valor para ellos mismos en mercados adyacentes aprovechando su dominancia en el mercado de su actividad principal.

56. Por último, por lo que nos interesa, el encargado debe diseñar sus sistemas de IA teniendo en cuenta los riesgos que pueden entrañar en colisión con los derechos fundamentales, ya que él es el que los conoce con mayor exactitud (*ex* art. 24 RGPD). En este punto las exigencias del RGPD parecen insuficientes puesto que no parece razonable, por ejemplo, que se incorporen datos personales del usuario en sistemas de *deep learning* sin que el consumidor manifieste, de nuevo, consentimiento para que se produzca esta operación.

57. Hasta un cierto punto, la Propuesta del Reglamento de IA por parte de la Comisión Europea presentada el 21 de abril de 2021 reconoce esta falta de regulación que suponen una verdadera amenaza a esta protección reforzada de la que se trata de dotar a la persona física a través del RGPD. La propuesta distingue entre distintos tipos de sistemas según el tipo de datos que se manejan en la tecnología de la que se trate; algunos de ellos están prohibidos (por ejemplo, los que son susceptibles de manipular el comportamiento humano), y otros están permitidos pero su actividad se verá limitada en función de un riesgo alto (por ejemplo, sistemas de identificación y categorización biométrica) o medio/bajo (asistentes virtuales).

58. Sin embargo, las soluciones formuladas están lejos de materializarse, y la única protección que se le otorga a la persona física en esta manifestación tecnológica se da por vía del RGPD, que solamente exige que el responsable del tratamiento considere las posibles implicaciones del sistema de IA respecto a su colisión con los derechos fundamentales del titular.

59. Aunque el RGPD en su conjunto da una respuesta regulatoria modernizada a los retos del ámbito de protección del consumidor en relación con sus datos personales capturando en mayor o menor medida las tecnologías emergentes, quedan grandes riesgos y problemas que no se atajan desde la perspectiva regulatoria y que deben atenderse mediante otras vías. Nosotros proponemos que dicha solución puede provenir desde el Derecho de la Competencia.

2. ¿Regulación ex ante o intervención ex post?

60. Hasta hace muy poco tiempo, el *Big Data* se ha venido analizando de forma fragmentaria[76]. Por una parte, las agencias de protección de datos realizan su análisis exclusivamente basadas en las premisas y principios del RGPD y de las normativas nacionales correspondientes en esta materia. Por otra parte, las autoridades de competencia han ignorado -hasta la fecha- estos razonamientos en sus evaluaciones y se han centrado en el análisis del daño competitivo, sin prever la posibilidad de que este perjuicio también se puede producir mediante un ataque injustificado a la privacidad de sus usuarios[77]. Existe un curso paralelo entre las líneas de actuación de ambas esferas para atajar una misma preocupación: 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[78].

[76] European data protection supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, marzo 2014, pp. 1-41 (pp. 6-7); T. De La Quadra-Salcedo Fernández Del Castillo, *"Cap. 1. Retos, riesgos y oportunidades de la sociedad digital"*, en T. De La Quadra Salcedo Y J.L. Piñar Mañas, *Sociedad digital y Derecho*, Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 21- 87 (pp. 63- 65).

[77] E. Ferrer Y A. Pol, "Capítulo 5. Protección de datos y derecho de la competencia", en M.A. Recuerda Girela (Dir), *Anuario de Derecho de la Competencia*, Ed. Civitas, Madrid, 2020, pp. 119-142.

[78] D.D. Sokol y R. Comerford, "Antitrust and Regulating Big Data", *George Mason Law Review*, 119 (23), septiembre 2016, pp. 1129-1161 (pp. 1133-1140).

61. Ohlhausen Y Okuliar, en un intento de explicar 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[79].

62. Partiendo de la concepción del *Big Data* como un *input* empresarial, señalan la complejidad metodológica con la que se enfrentan las autoridades de competencia nada más empezar su análisis: es complicado asociar un valor/precio concreto a los datos almacenados y procesados por una empresa en relación con el coste del servicio prestado. De esta forma, para analizar los riesgos anticompetitivos generados por el *Big Data* las autoridades de competencia deben forzar las herramientas de las que disponen para tratar de atajar el conjunto de problemas que se dan por su causa.

63. Ante esta complejidad, las autoridades de competencia tienden a prestar atención a una perspectiva estática de los mercados digitales, que es precisamente uno de los errores metodológicos básicos en su análisis[80]. Como se ha puesto de manifiesto, las autoridades de competencia, sobre apreciaciones subjetivas de este fenómeno, tratan de imponer presunciones de culpabilidad a las grandes plataformas digitales, tal y como podemos observar en el caso de los instrumentos propuestos por la Comisión Europea para combatir a los guardianes de acceso, a través de las obligaciones que se les imponen en la DMA.

64. 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 los usuarios de las plataformas digitales. 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 competente. Esta postura resulta cuanto 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, es decir, en beneficio de los propios consumidores.

65. A pesar de estas dificultades, el solapamiento entre las consideraciones de privacidad y *antitrust* ha ido en aumento, sobre todo en la práctica decisoria de la CE, y sin duda ninguna ambos enfoques están llamados a ser integrados en un único análisis. De hecho, ya existen novedosas propuestas doctrinales que sugieren analizar la protección de datos no desde la perspectiva de los derechos fundamentales, sino como fallo de mercado, que lleva a un abuso de posición dominante de los de la categoría de abusos explotativos[81]. Según estos autores, este enfoque permitiría integrar su evaluación como parámetro del proceso competitivo, al considerar las restricciones a la privacidad como una forma de abuso de explotación. Desde luego, parece claro que el papel en el ámbito del control de concentraciones de los datos ha ido en un patente *in crescendo*.

66. Así, en la operación *TomTom/TeleAtlas*, aprobada en 2008, se reconocieron -por primera vez- los datos como un parámetro de competencia, pero no se consideró la aplicación de la normativa de protección de datos a efectos del análisis competitivo[82]. Ese mismo año, la operación *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*»[83].

---

[79] M.K. Ohlhausen Y A.P. Okuliar, "Competition, consumer protection, and the right [approach] to privacy", *Antitrust Law Journal*, 80 (1), 2015, pp. 121-156.

[80] N. Petit Y D.J. Teece, "Innovating Big Tech Firms and Competition Policy: Favoring Dynamic Over Static Competition", *Industrial and Corporate Change*, marzo 2021, pp. 1-31 (pp. 4-6).

[81] N. Economides Y I. Lianos, "Restrictions on privacy and exploitation in the Digital Economy: A market failure perspective", *Journal of Competition Law & Economics*, 00(00), 2021, pp. 1-83.

[82] Decisión de la Comisión Europea de 14 de mayo de 2008, *TomTom / TeleAtlas*, Case nº COMP/M.854, C(2008) 1859.

[83] Decisión de la Comisión Europea de 11 de marzo de 2008, *Google /DoubleClick*, Case nº COMP/M.4731, C(2008) 927 final, par. 368.

67. Idéntica postura se adoptó en la operación *Facebook/WhatsApp* aprobada en 2014, en la que hay una cierta sensación de que la CE pecó de no haber dado a los datos y las consideraciones de privacidad la importancia que tenían, relegando esa valoración a las autoridades de protección de datos[84]).

68. No fue hasta el 2016 con la operación *Microsoft/LinkedIn* en que se sentaron las bases para un cambio de paradigma[85]. 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[86]. 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.

69. Como es lógico en este tipo de supuestos, la CE 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[87]. 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 *Apple/Shazam*[88].

70. ¿Cómo establecer el adecuado equilibrio entre protección de la privacidad y protección de la competencia? ¿Hasta qué punto pueden las consideraciones sobre privacidad y protección de datos constituir un parámetro del proceso competitivo? En el marco de este binomio examinaremos en el epígrafe IV casuísticamente aquellos hitos que se han dado en la práctica decisoria de las autoridades *antitrust* como intentos por aproximar ambas materias.

3. Herramientas y dificultades del Derecho de la Competencia

71. Como paso previo a realizar dicho 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 sancionadora que atiende a la conducta de los competidores en el mercado, ya sea a través de acuerdos entre ellos -prácticas colusorias-, prohibidas por el art. 101 TFUE o bien porque uno de ellos se prevalece de su posición de dominio en el mercado -abuso de posición dominante-, prohibido por el art. 102 TFUE.

72. 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) nº 139/2004 del Consejo, de 20 de enero de 2004, sobre el control de las concentraciones entre empresas[89].

---

[84] Decisión de la Comisión Europea de 13 de octubre de 2014, *Facebook/WhatsApp,* Case nº COMP/M.7217, C(2014) 7239 final, par. 164; *Vid.*, entre otros, R. Allendesalazar, "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, noviembre de 2020, pp. 1-38 (p. 425).

[85] Decisión de la Comisión Europea de 6 de diciembre de 2016, *Microsoft/LinkedIn,* Case nº COMP/M.8124, C(2016) 8404 final.

[86] Decisión de la Comisión Europea de 6 de diciembre de 2016, *Microsoft/LinkedIn,* Case nº COMP/M.8124, C(2016) 8404 final, pars. 255 y 350.

[87] C. Herrero Suárez, "Cap. 31. Big Data y Derecho de la Competencia*"*, en T. De La Quadra Salcedo Y J.L. Piñar Mañas (Coord.), *Sociedad digital y Derecho,* Madrid, Red. es y Boletín Oficial del Estado, 2018, pp. 659-683 (pp. 673 a 680).

[88] Decisión de la Comisión Europea de 6 de septiembre de 2018, *Apple/Shazam,* Case M. 8788, C(2018) 5748 final.

[89] Reglamento (CE) nº 139/2004 del Consejo de 20 de enero de 2004 sobre el control de concentraciones entre empresas, *DOUE* L 024, 29 de enero de 2004, p. 1-22.

73. 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.

74. A partir de este instrumental del que disponen las autoridades de competencia, lo que ya nadie parece poner en duda es que los datos son una fuente de poder de mercado[90]. En efecto, la obtención, almacenamiento y procesamiento de los datos personales han dejado de ser cuestiones sometidas a las restricciones legales orientadas a la protección de la privacidad para convertirse en un parámetro de la competencia, no basado en precios sino en la calidad del servicio[91], que es especialmente acusado en aquellos servicios que se prestan a precio cero a los consumidores y usuarios[92].

75. Así, en los mercados impulsados por esta nueva economía de los datos, estos constituyen una ventaja competitiva que se traduce en una fuente de poder de mercado. De ahí que las empresas tengan un incentivo para implementar estrategias de protección de datos que les sirvan para crear o reforzar una posición dominante en el mercado[93], ya sea con un aumento o una disminución de los niveles de protección en la recogida y procesamiento de los datos de sus usuarios, o de empresas que operan en sus plataformas.

76. Por un lado, la disminución de la protección de la privacidad podría constituir un abuso de explotación a los usuarios finales, como veremos en el apartado siguiente que consideró la FCO (autoridad alemana de la competencia en el caso *Facebook*). Por otro lado, el aumento de la protección de la privacidad podría excluir o discriminar a los rivales, tal y como alegan los demandantes en las investigaciones alemanas y francesas sobre la transparencia del seguimiento de las aplicaciones de *Apple* (ATT).

77. Desde la óptica del Derecho de la Competencia evaluar la privacidad como parámetro competitivo conlleva una dificultad evidente: a diferencia del precio, esa degradación de la calidad del servicio que el cliente puede percibir cuando se rebaja la protección de la privacidad es, por su misma naturaleza, subjetiva, no cuantificable, multidimensional, y enteramente dependiente de la personal sensibilidad de cada consumidor. Si a esto añadimos la existencia de la *privacy paradox*, a la que nos referiremos en adelante, no es difícil darse cuenta de las enormes dificultades a las que se enfrenta el análisis del Derecho de la competencia en esta materia.

---

[90] L.M.B. Cabral, J. Haucap, G. Parker, G. Petropoulos, T.M. Valletti y M.W. van alstyne, "The EU Digital Markets Act: A Report from a Panel of Economic Experts", *Publications Office of the European Union*, JRC122910, 2021, pp. 1-36 (p. 20).

[91] R. Lande, "The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern*"*, *FTC: Watch*, No. 714, 2008; N. Just, "Governing Online Platforms: Competition Policy in Times of Platformization*"*, *Telecommunications Policy*, 42 (5), junio 2018, pp. 386-394 (pp. 386-388).

[92] Directorate for financial and enterprise affairs (Competition Committee), "Quality considerations in digital zero-price markets—Background note by the Secretariat", 9 de octubre de 2018, DAF/COMP(2018)14, pp. 1-46 (pp 6-8).

[93] Así es como se entiende en artículos doctrinales y comentarios recientes, y no se duda en calificar la protección de la privacidad como un pretexto para lo que realmente se pretende: la puesta en práctica de políticas anticompetitivas. *Vid.*, a modo de ejemplo: D. Sokol Y F. Zhu, "Harming Competition and Consumers Under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates", *University of Southern California,* USC CLASS Research Paper No. CLASS21-27, junio 2021, pp. 1-23.

78. Para hacer frente a esta dificultad, además de refinar el instrumental con el que actualmente contamos, para adaptarlo a esta nueva perspectiva híbrida -regulación y competencia-, habría que articular igualmente algún tipo de cooperación entre las respectivas autoridades, las que protegen la privacidad y los datos personales (en España, por ejemplo, la AEPD, *Agencia Española de Protección de Datos*) y las que tutelan la libre competencia en el mercado (en España, la CNMC, *Comisión Nacional de los Mercados y la Competencia*). A este respecto, hay ya aportaciones doctrinales que proponen esta cooperación institucional, al hilo del estudio de un fenómeno -la publicidad personalizada, o *targeted advertising*- que evidencia este doble aspecto de los datos: su valor personal para el consumidor y su valor económico para las plataformas digitales[94].

79. Posiblemente el mejor ejemplo de que este tipo de cooperación es posible, y las evidentes ventajas en términos de un *enforcement* que integre ambos enfoques, es la reciente declaración conjunta de la autoridad de protección de datos -*Information Commissioner's Office* (ICO)- y de la competencia -*Competition and Markets Authority* (CMA)- en Reino Unido, al que hemos hecho ya reiteradas referencias en epígrafes precedentes, y que pone de manifiesto la pretendida contraposición entre los objetivos de uno y otro ordenamiento, así como las indudables sinergias y ventajas que se derivan de este enfoque integrador que estamos proponiendo en estas páginas: «*Los objetivos del derecho de la competencia y de la protección de datos se han caracterizado en ocasiones como objetivos opuestos. No estamos de acuerdo. Hay sinergias fundamentales que sustentan nuestros respectivos objetivos políticos y creemos que aunque puedan surgir tensiones, son superables*»[95].

80. Desde fechas tempranas encontramos pronunciamientos tanto de autoridades de competencia como de protección de datos en la dirección de integrar ambos aspectos. Así, ya en 2014 la Agencia Europea de Protección de Datos había manifestado que en los mercados digitales el almacenamiento y ulterior procesamiento de los datos era una fuente de poder de mercado[96]. Algo parecido manifestó la propia OCDE dos años más tarde[97].

81. Asimismo, el consenso doctrinal es cada vez mayor en relación con el peculiar poder de mercado derivado de los datos y en la economía digital. Según este modelo de negocio de las nuevas plataformas, las herramientas clásicas del Derecho de la Competencia se quedan atrás para abarcar el conjunto de su extensión[98]. es difícilmente cuantificable y "manejable" por las herramientas clásicas que el Derecho de la Competencia tradicionalmente ha empleado en mercados analógicos

82. Como veremos en el epígrafe siguiente, al hilo de asuntos recientes que han resuelto las autoridades europeas y estadounidenses, el enfoque conjunto privacidad-competencia no está, ni mucho menos, conseguido. Tanto en el ámbito del control de concentraciones, como en el de considerar prácticas restrictivas de la privacidad o la acumulación excesiva de datos como nuevas tipologías del abuso de posición dominante, la praxis decisoria es vacilante, ambigua, cuando no errática y contradictoria.

---

[94] J. Tamayo Velasco, "Big Data, Competencia y Protección de Datos: el Rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada", *Revista de Estudios Europeos*, nº 78, Julio-diciembre 2021, pp. 183-202.

[95] Competition & Markets Authority y Information Commissioner's Office., *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 de mayo de 2021, pp. 1-31 (p. 18).

[96] European data protection supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, marzo 2014, pp. 1-41 (p. 28).

[97] Directorate for Financial and Enterprise Affairs (Competition Committee), *Big Data: bringing competition policy into the digital era*, 27 de octubre de 2016, DAF/COMP(2016)14, pp. 1-40 (p. 16).

[98] *Vid.*, por todos, V.H.S.E. Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Common Market Law Review*, 57, 2020, pp. 161–189.

IV. Las autoridades de competencia ante el Big Data en los mercados digitales

1. La operación de concentración Google/Fitbit

83. 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*»[99].

84. En efecto, ante la propuesta de adquisición de *Fitbit* por parte de *Google*[100], cuyo análisis recayó en la Comisión Europea, la autoridad comunitaria manifestó en primera fase su preocupación por el posible impacto de la operación, teniendo en cuenta la posición dominante (además de sus economías de escala y alcance) que *Google* ya ostentaba en el mercado de las búsquedas online en el mercado interior común.

85. La entidad resultante de la fusión tendría acceso al *Big Data* de *Fitbit,* que contiene sobre todo datos sanitarios 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, 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).

86. Paralelamente, los operadores del mercado ,a las autoridades de protección de datos y las autoridades de competencia consultadas 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[101]. 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.

87. Teniendo en cuenta todo ello, la Comisión Europea dio paso a la segunda fase de la evaluación. 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*.

88. En este sentido, la Comisaria Vestager afirmó 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*»[102]. 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*[103].

---

[99] Speech – Margrethe Vestager: "Clearing the path for Innovation", Web Summit, Lisboa, 7 de noviembre de 2017.

[100] Company Announcements - Rick Osterloh (Senior Vice President, Devices & Services de Google): "Helping more people with wearables: Google to acquire Fitbit", The Keyword, 1 de noviembre de 2019.

[101] En particular, la autoridad australiana de competencia había indicado que existe una fuerte interacción entre los datos y la competencia. *Vid.* por todos: Australian Competition & Consumer Commission, Statement of Issues, 18 June 2020, *Google LLC-proposed acquisition of Fitbit Inc*, pp. 1-25.

[102] Press release – European Commission: "Mergers: Commission opens in-depth investigation into the proposed acquisition of Fitbit by Google", Bruselas, 4 de agosto de 2020, IP/20/1446.

[103] Press release – European Data Protection Board: "Eighteenth EDPB Plenary Session", 20 de febrero de 2020, EDPB_PressRelease_2020_02.

89. Una vez concluidas sus investigaciones, la CE 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*.

90. En el comunicado de prensa en el que hizo pública su decisión, la CE 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 reguladoras 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*»[104]. Aunque soterradamente la CE *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.

91. Naturalmente, este enfoque tan favorable a la operación que considera a esta exenta de riesgos para el mercado y para los consumidores no es compartida por todos. Sirva como botón de muestra el informe publicado por el Centre For Economic Policy Research, enormemente crítico con la autorización de esta operación de concentración[105]. En su opinión, esta supone un daño directo a los consumidores, un fortalecimiento de 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.

92. 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 «*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![106] (o al menos debe intentar integrarse dentro del marco del análisis de competencia, como han planteado algunas autoridades de competencia).

2. El caso Bundeskartellamt c. Facebook

93. La interacción de la privacidad de los usuarios de las plataformas digitales y el Derecho de la Competencia se ha planteado ya, y de forma palmaria, como teoría del daño ante la autoridad alemana de competencia. En concreto, el caso se planteó en relación con la imposición de términos y condiciones

[104] Press release -European Commission: "Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions", Bruselas, 17 de diciembre de 2020, IP 20/2484.

[105] Centre for Economic Policy Research, "Google/Fitbit will monetise health data and harm consumers", *CEPR Policy Insight,* nº107, septiembre 2020, pp. 1-13.

[106] Y así se manifiesta desde la doctrina más autorizada. *Vid*, entre otros: C. Caffarra Y T. Valetti, "Google/Fitbit review: Privacy IS a competition issue", *Voxeu Competition Report*, 4 de marzo de 2020.

(TyC) a los usuarios de plataformas digitales como puerta de acceso a la prestación de sus servicios. En el marco de la prohibición de abuso de posición dominante de la Ley alemana (GWB)[107], la autoridad de competencia -*Federal Cartel Office* (FCO) o *Bundeskartellamt*- planteó la posible introducción de los parámetros de privacidad como un elemento de competencia. Como se ha apuntado desde algún sector doctrinal, este caso además consideró la protección de los consumidores -su privacidad, sus datos personales- como una de las finalidades también del Derecho de la competencia, más allá de las consideraciones puramente regulatorias en materia de protección de datos[108].

A) La decisión de la autoridad de competencia alemana

94. La FCO comenzó a investigar en 2016 si *Facebook* estaba abusando de su posición dominante en el mercado de las redes sociales a través de la imposición de cláusulas contractuales abusivas en sus términos y condiciones[109]. La política de privacidad de la empresa estaba diseñada con el mecanismo de *opt-in*, es decir, si los usuarios no mostraban su conformidad a los términos impuestos por *Facebook* no podrían acceder a ninguno de los servicios ofrecidos por la red social. Por tanto, la decisión del usuario se veía reducida a la mínima expresión, y solamente podrían aceptar los términos y condiciones si querían acceder al servicio[110].

95. En concreto, el presidente de la FCO Andreas Mundt afirmó que «*las empresas dominantes en el mercado están sujetas al cumplimiento de obligaciones específicas. Estas obligaciones comprenden el uso de términos y condiciones adecuados al servicio que prestan, siempre que sean necesarias y relevantes en el mercado en el que operan. Para aquellos servicios prestados online cuyo volumen de negocios depende de sus anunciantes como es el caso de Facebook, los datos de sus usuarios son especialmente valiosos. Por este motivo, es esencial que se examine en el marco del análisis del abuso de posición dominante si los consumidores han sido informados suficientemente sobre el tipo y alcance de la recopilación de datos que la plataforma va a utilizar para su posterior tratamiento*»[111].

96. La FCO analizó detalladamente los TyC de los servicios ofrecidos por *Facebook*, concluyendo que el tratamiento integral de dichos datos personales infringía el RGPD. Esta afirmación viene precedida de una consulta a la autoridad de protección de datos, con la que colabora la autoridad en este asunto. Tal y como señala en su consulta a la autoridad de protección de datos, esta considera que la autoridad de competencia está legitimada para aplicar los principios instituidos por el RGPD en el marco de la evaluación de la conducta de la empresa dominante[112].

97. Sobre la base del art. 8 CDFUE, la FCO considera que el consentimiento que prestaron los usuarios de *Facebook* en sus TyC está viciado, ya que estos no eran plenamente conscientes de las tareas de recogida y tratamiento de datos que se iban a realizar por parte de la red social. En paralelo, la autoridad incide en que, aun en el supuesto en que se considerar que se ha prestado ese consentimiento

---

[107] Conviene hacer notar aquí que, a diferencia de lo previsto en el art. 102 TFUE, o en la mayoría de las legislaciones de los estados miembros, como por ejemplo nuestra Ley 15/2007, de Defensa de la Competencia, el párrafo 18.3 (a) de la *Gesetz gegen Wettbewerbsbeschränkungen* explícitamente hace referencia a los datos como fuente de poder de mercado.

[108] V.H.S.E. Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Common Market Law Review*, 57, 2020, pp. 161–189 (pp. 168-175).

[109] N.M. Volmara y O.K. Helmdachb, "Protecting consumer and their data trough competition law? Rethinking abuse of dominance in light of Federal Cartel Office's Facebook investigation*", European Competition Journal*, Vol. 14 (2-3), 2018, pp. 195-215.

[110] Competition & Markets Authority y Information Commissioner's Office., *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 de mayo de 2021, pp. 1-31 (p. 19).

[111] News – Bundeskartellamt: "Bundeskartallemt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules", 2 de marzo de 2016.

[112] G. Colangelo Y M. Maggiolino, "Antitrust über alles. Whither Competition Law after Facebook*?", World Competition Law and Economic Review*, 42(3), 2019, pp. 1-18 (p. 8).

libremente, la cantidad de datos recopilada es excesiva y no es necesaria para la actividad de *profiling* realizada por *Facebook*[113].

98. Una vez sentado que *Facebook* recogía ilegalmente los datos personales de sus usuarios para mejorar sus propios servicios de publicidad personalizada por el primer motivo y el segundo que hemos expuesto, la FCO determinó que los usuarios perdían el control sobre sus datos personales, de forma contraria a lo exigido por el RGPD.

99. De esta forma, *Facebook* consolidaba su posición de dominio frente al resto de sus competidores, fortaleciendo las barreras de entrada al mercado de las redes sociales[114]. En su análisis, la FCO determinó que dichas barreras de entrada estaban reforzadas por la imposibilidad de los competidores de reproducir la base de datos que *Facebook* había obtenido en aplicación de su política de TyC[115], cuyos efectos ni siquiera podrían verse contrarrestados por la presión competitiva de la innovación en Internet ni la ejercida por los escasos y débiles competidores que tenía en el mercado[116].

100. Todo ello condujo a la autoridad alemana a determinar en junio de 2019, que los TyC impuestos a los usuarios de *Facebook* eran cláusulas contractuales abusivas. Y en la medida en que está práctica era una manifestación directa del poder de mercado de la popular empresa, la FCO confirmó el abuso por parte de *Facebook* de su posición de dominio en el mercado de las redes sociales privadas[117]. Como hemos señalado, esta decisión es ciertamente histórica, ya que es la primera vez que una conducta basada en la imposición de una política de privacidad contraria al RGPD se considera como práctica abusiva según el Derecho de la Competencia.

101. Naturalmente, hay aspectos cuestionables: en primer lugar, la falta de parámetros objetivos de la decisión, ya que el valor que los usuarios atribuyen a sus propios datos, y por tanto a las condiciones de su recopilación -y en general a su tratamiento- es extremadamente variable, y en algunos casos, hasta inexistente. De ahí que admitir la existencia de un abuso llevado a cabo a través de la política de privacidad de *Facebook,* supondría admitir la existencia de condiciones contractuales *per se* abusivas, (que no son percibidas como tales por los usuarios), desvirtuando así la propia función del Derecho *antitrust*, es decir, la protección del bienestar social.

102. En segundo lugar, desde un punto de vista sistemático, la sanción por abuso de posición dominante no resuelve los posibles efectos excluyentes sobre la competencia que se generaron a través de la exigencia de la prestación de consentimiento en el seno de sus términos y condiciones. *Facebook* podría adecuar el tratamiento de los datos al RGPD y, sin embargo, recopilar la misma cantidad de datos sin que le sea reprochable dicha conducta ni desde la normativa de protección de datos ni desde el Derecho de la Competencia, aunque siga persistiendo ese supuesto daño anticompetitivo que se ha generado en el mercado de las redes sociales.

103. En tercer lugar, la decisión adoptada por la FCO omite una de las principales eficiencias generadas por el uso del *Big Data*, a la que hemos hecho referencia: la creación de nuevos servicios o

[113] Según la FCO, aunque los anuncios mostrados podrían ser menos eficaces y precisos, *Facebook* seguiría siendo capaz de prestar el servicio de perfilación de usuarios a los anunciantes. *Vid.* Decisión del Bundeskartellamt de 6 de febrero de 2019, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB por inadequate data processing*, Ref. B6-22/16, par. 695.

[114] Decisión del Bundeskartellamt de 6 de febrero de 2019, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB por inadequate data processing*, Ref. B6-22/16, pars. 452-480.

[115] Decisión del Bundeskartellamt de 6 de febrero de 2019, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB por inadequate data processing*, Ref. B6-22/16, pars. 469-472.

[116] Decisión del Bundeskartellamt de 6 de febrero de 2019, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB por inadequate data processing*, Ref. B6-22/16, pars. 501-521.

[117] Decisión del Bundeskartellamt de 6 de febrero de 2019, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB por inadequate data processing*, Ref. B6-22/16*,* par. 873.

la mejora de los existentes que satisfacen la demanda de sus usuarios, en términos del Derecho de la Competencia. Habiéndolo omitido, resulta algo forzado señalar que la conducta de *Facebook* tiene un efecto anticompetitivo[118].

B) Suspensión de la decisión en primera instancia en sede cautelar

104. Resolviendo el recurso interpuesto por *Facebook*, el Tribunal Superior Regional de Düsseldorf (OLG) suspendió cautelarmente la decisión de la FCO, al apreciar que la teoría del daño construida 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*»[119]. 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[120].

105. 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[121].

106. En la línea de la discusión que venimos analizando, el Tribunal considera que la autoridad alemana de competencia utilizó las herramientas de competencia -en este caso la prohibición de abuso de posición dominante- para tratar de justificar su competencia en una materia que corresponde en exclusiva a las autoridades de protección de datos. En palabras del OLG, la FCO «*está analizando exclusivamente un problema de protección de los datos personales y no uno de falta de competencia en los mercados*»[122]. En este sentido, el simple hecho de que *Facebook* tuviera un altísimo número de usuarios activos a diario en la red social no podía considerarse prueba suficiente para establecer que los usuarios perdieron el control sobre sus datos. Por lo tanto, el OLG concluye que la cuestión sobre si el consumidor medio tenía todos los instrumentos a su disposición para entender en profundidad el poder que le otorgaba a *Facebook* aceptando sus TyC, nada tiene que ver con el Derecho de la Competencia.

C) Pronunciamiento sobre la decisión en segunda instancia en sede cautelar

107. Recurridas las conclusiones alcanzadas por el OLG, en junio de 2020 el Tribunal Federal de Justicia alemán (BHG) revocó 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[123].

---

[118] G. Colangelo y M. Maggiolino, "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S.", *Stanford Law School and the University of Vienna School of Law TTLF,*. Working Paper No. 31, 2018, pp. 1-46.

[119] Decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, 26 August 2019, Case VI-Kart 1/19 (V), pp. 1-31 (p. 6).

[120] Decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, 26 August 2019, Case VI-Kart 1/19 (V), pp. 1-31 (p. 7).

[121] Decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, 26 August 2019, Case VI-Kart 1/19 (V), pp. 1-31 (p. 9).

[122] Decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, 26 August 2019, Case VI-Kart 1/19 (V), pp. 1-31 (p. 10).

[123] Press release – Federal Court of Justice (Bundesgerichtshof): "Federal Court of Justice provisionally confirms allegation of Facebook abusing dominant position", 23 de junio de 2020, No. 080/2020.

108. El BHG, sin embargo, transforma la decisión de la FCO y le otorga un nuevo sentido. Por un lado, según el Tribunal, lo que resulta decisivo para imputar un abuso de posición no es la infracción del RGPD por parte de *Facebook,* sino los TyC abusivos que se impusieron a sus usuarios en relación con el tratamiento de sus datos. El BHG cifra dicha abusividad en que la red social no permitiera a sus usuarios elegir el grado de intensidad -pudiendo modular la cantidad de datos personales que se facilitaban- de la recopilación y tratamiento de datos que se iba a realizar a efectos de la tarea de *profiling*. Añade, además, que si *Facebook* tuviera competidores reales en el mercado no podría imponer estas condiciones, porque los usuarios elegirían servicios menos invasivos de su privacidad.

109. Esta conclusión parece distanciarse de la realidad empírica, que demuestra que a pesar de que los usuarios de plataformas digitales expresen una preferencia clara por una mayor protección de sus datos personales, suelen consentir a un tratamiento mucho más intensivo que aquel que desearían, lo que se denomina la *privacy paradox*[124]. En su decisión el BHG obvia que los consumidores tienen la posibilidad, en todo caso, de elegir no utilizar la red social si deciden que los TyC son inaceptables.

110. Partiendo de todo ello, el BHG acoge la teoría del daño esbozada inicialmente por la FCO, y añade que la conducta de *Facebook* no solamente refuerza su posición en el mercado de la publicidad online, sino también en el mercado conexo de las redes sociales[125]. Mediante la técnica de *profiling, Facebook* consigue mejorar la experiencia personalizada del usuario en sus propios servicios y, atraídos por este incremento en la calidad del servicio, estos permanecen un mayor tiempo en la red social. En el momento en que se escriben estas líneas, y tras varios recursos y el planteamiento por parte del *Düsseldorf Higher Regional Court* de una cuestión prejudicial ante el TJUE, el caso está aún sin un pronunciamiento definitivo[126].

3. La perspectiva estadounidense

111. 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 EE.UU. 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 *Facebook,* exactamente por la misma práctica de abuso de posición dominante (si utilizamos sus términos, *monopolization,* sancionada por la Sección 2ª de la *Sherman Act*).

112. 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 versan en conductas que sólo resultarían perjudiciales para los consumidores[127]. El Informe asume que las *GAFA* (y sólo ellas) han incurrido en prácticas anticompetitivas como el auto favorecimiento de sus productos (es decir, aprovechar su condición de guardianes de acceso 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

[124] A. Acquisti, *"Nudging Privacy: The Behavioral Economics of Personal Information", Digital Enlightenment Yearbook*, 2012.

[125] Decisión del BGH (Bundesgerichtshof) de 23 de junio de 2020, *Facebook,* KVR 69/19.

[126] R. Podszun, "Facebook: Next Stop Europe", *D'Kart blog*, 25 de marzo de 2021, disponible en: https://www.d-kart.de/en/blog/2021/03/25/facebook-next-stop-europe/ (última consulta el 30 de noviembre de 2021)

[127] M. López-Galdós, "The HJC Report on the Future of the U.S. Competition System: Part 1", *Disruptive Competition Project*, 6 de octubre de 2020, disponible en: https://www.project-disco.org/competition/100620-the-hjc-report-on-the-future-of-the-u-s-competition-system-part-1/ (última consulta el 30 de noviembre de 2021).

(*killer acquisitions*, en los términos del ámbito del control de concentraciones), el uso indebido de los datos recopilados y la creación de barreras de entrada en el mercado.

113. 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 EE.UU. no han podido frenar estas prácticas anticompetitivas hasta el momento, también por una falta acuciante de recursos materiales y humanos.

A) El DOJ (y otros Estados) c. Google

114. Poco después de la publicación de este Informe, el Departamento de Justicia de los Estados Unidos (DOJ en adelante) presentó una demanda contra *Alphabet Inc.*, la empresa matriz de *Google*, por *monopolización*[128].

115. El núcleo de la demanda estriba en los contratos de distribución 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*[129]. 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 cuasi-monopolista (recordemos que *Google* tiene en EE. UU. una cuota en torno al 90% en el mercado de las búsquedas online).

116. El punto de partida de la demanda del DOJ, y aquí es patente el paralelismo con el planteamiento asumido por la CE en la DMA, es que *Google* es un guardián de acceso y además 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*». Naturalmente, la empresa se aprestó a calificar la demanda como infundada[130], y que no beneficiaba a los consumidores, y ha sido ya objeto de múltiples análisis[131].

117. A diferencia de la UE, 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 contra *Facebook* pocos días después, esta vez por la FTC[132].

---

[128] United States District Court for the District of Columbia, Complaint *United States of America, State of Arkansas, State of Florida, State of Georgia, State of Indiana, Commonwealth of Kentucky, State of Louisiana, State of Mississippi, State of Missouri, State of Montana, State of South Carolina and State of Texas v. Google LLC*, filed 20 October 2020, Case 1:20-cv-03010,

[129] Esta parte del expediente es exactamente igual al seguido en la UE años antes: Decisión de la Comisión Europea de 18 de julio de 2018, *Google Android,* Case AT.40099, C(2018) 4761 final.

[130] Public policy – Google (Kent Walker, SVP of Global Affairs): "A deeply flawed lawsuit that would do nothing to help consumers", 20 de octubre de 2020.

[131] *Vid*., entre otros, D. Geradin, "The U.S. v. Google: A preliminary analysis in ten points", *The Platform Law Blog,* 21 de octubre de 2020, disponible en: https://theplatformlaw.blog/2020/10/21/the-u-s-v-*Google*-a-preliminary-analysis-in-ten-points/amp/ (última consulta el 30 de noviembre de 2021).

[132] United States District Court for the District of Columbia, Complaint for injunctive and other equitable relief, filed 13 January 2021, *Federal Trade Commission v. Facebook, Inc.*, Case No.: 1:20-cv-03590.

B) La Federal Trade Commission c. Facebook: un viaje de ida y vuelta

118. 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%.

119. 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 que no contarán con este número de usuarios).

120. 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*.

121. 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[133].

122. 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*». 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 de 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.*...»).

123. 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 EE.UU. 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.

[133] N. Petit Y D.J. Teece, "Innovating Big Tech Firms and Competition Policy: Favoring Dynamic Over Static Competition", *Industrial and Corporate Change*, marzo 2021, pp. 1-31 (pp. 28-31).

124. 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 la que las autoridades tratan de remediar los grandes abusos potenciados por los efectos de red de estas grandes empresas tecnológicas.

125. La desestimación de la demanda en sede preliminar del juez de Washington James Boasberg el pasado 28 de junio de 2021 se basó en la incorrecta definición de la posición dominante de *Facebook*. Ello llevó a que el pasado 17 de noviembre de 2021, la autoridad *antitrust* norteamericana planteara una segunda demanda, por lo que, como puede apreciarse, el litigio está lejos de concluir[134].

V. Conclusiones

126. 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.

127. 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, los textos fundacionales de la Unión Europea, así como en su regulación en forma de Derecho derivado mediante el RGPD.

128. 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 CE publicó su propuesta de Reglamento sobre la IA.

129. 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

[134] United States District Court for the District of Columbia, Plaintiff Federal Trade Commission's Memorandum of Law in Opposition to defendant Facebook, Inc.'s motion to dismiss amended complaint, filed 17 November 2021, *Federal Trade Commission v. Facebook, Inc.,*, Civil Action No. 1:20-cv-03590 (JEB).

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.

130. 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 EE.UU. 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.

131. 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, a pesar de que se produzca, *de facto,* la *privacy paradox.*