Revista de Estudios Europeos
Nº 78, julio-diciembre, 2021, 183-202
ISSN: 2530-9854. http://www.ree-uva.es/

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

BIG DATA, COMPETITION POLICY AND DATA PROTECTION: THE ROLE OF THE GENERAL DATA PROTECTION REGULATION IN TARGETED ADVERTISING BUSINESS MODELS

Jimena TAMAYO VELASCO
Universidad de Valladolid

Resumen: En el marco de la economía de los datos, han florecido modelos de negocio basados en la publicidad personalizada que sustentan plataformas como Google o Facebook. Partiendo de la naturaleza dual de los datos, el presente trabajo estudia cómo el Reglamento General de Protección de Datos puede constituir un instrumento útil a efectos de limitar los abusos anticompetitivos en que puedan incurrir estos guardianes de acceso. Pese al interés teórico del Reglamento, se argumentará que, en último término, el control o soberanía de los usuarios finales sobre sus datos podría disminuir su efectividad en la práctica.

Palabras: clave. Big data, Google, Facebook, publicidad personalizada, consentimiento informado, portabilidad de datos.

Abstract: The data economy has allowed for the flourishing of targeted advertising business models, supported by platforms such as Google or Facebook. Departing from the dual nature of data, this work aims at studying how the General Data Protection Regulation could be a useful tool in order to limit the anti-competitive abuses that these gatekeepers may commit. Despite the theoretical interest of the Regulation, it will be argued that, ultimately, the sovereignty of end users over their data could reduce its effectiveness in practice.

Keywords: Big data, Google, Facebook, targeted advertising, informed consent, data portability.

1. Conceptos previos: mercados digitales, modelos de negocio basados en la publicidad personalizada y el valor de los datos

"When advertising is involved you the user are the product".[1] Esta advertencia –manifestada por los fundadores de *Whatsapp* en 2012, antes de caer en las manos de *Facebook*– condensa el significado de los modelos de negocio basados en la publicidad personalizada que se han desarrollado en el marco de la floreciente economía de los datos.

La publicidad *online* es uno entre tantos mercados digitales acaparados en su práctica totalidad por cuatro gigantes tecnológicos: *Google, Facebook, Amazon* y *Apple.* Las sólidas posiciones de dominio de que disfrutan estas "plataformas digitales" no dejan de levantar sospechas, encontrándose bajo el escrutinio de las autoridades de competencia alrededor de todo el mundo.

Ciertamente, la existencia de fuertes barreras de entrada a estos mercados justificaría en parte su tendencia a la concentración. Efectos de red directos e indirectos, elevados costes de cambio, economías de escala y de alcance, fuertes costes fijos y, por supuesto, la ventaja competitiva que ofrece el *big data*, son las más significativas.[2] Estas características propias e inherentes a los mercados digitales generan una dinámica en la que la competencia se produce *por* el mercado y no *en* el mercado. En otras palabras, "el ganador se lleva todo" *(winner-takes-it-all*).[3]

No obstante, la monopolización de sectores podría verse facilitada por las conductas anticompetitivas de las plataformas que los controlan: adquisiciones estratégicas –entre las que se incluyen las peligrosas *killer acquisitions*, letales para la innovación–,[4] configuración predeterminada (*default setting*) y favorecimiento (*self-preferencing*) de sus propios servicios, precios predatorios, prácticas de vinculación, etc.

Google y *Facebook* –reuniendo, conjuntamente, el 99% del incremento interanual de los ingresos procedentes de este sector en Estados Unidos en 2017–[5] disfrutarían de lo que algunos definen como un "duopolio" en el mercado de la publicidad *online*.[6] A su vez, cada una de estas empresas monopoliza otros mercados digitales adyacentes. *Google* es la indudable vencedora en el mercado de los buscadores de internet, mientras que *Facebook* –gracias, entre otras cosas, a la

1 Whatsapp (2012): "Why we don't sell ads". *Whatsapp*. Disponible en: https://blog.whatsapp.com/why-we-don-t-sell-ads [consulta: 08-04-2021].
2 Subcommittee on Antitrust, Commercial and Administrative Law of The Committee on The Judiciary (2020): *Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations*. House of Representatives. United States, pp. 40-46.
3 *Ibid*, p. 37.
4 *Ibid*, p. 38.
5 Heath, A. (2017): "Facebook and Google Completely Dominate the Digital Ad Industry". *Business Insider*. Disponible en: https://www.businessinsider.com/facebook-and-google-dominate-ad-industry-with-a-combined-99-of-growth-2017-4 [consulta: 08-04-2021].
6 Subcommittee on Antitrust (…), *Investigation of Competition… cit.*, p. 171.

adquisición de *Instagram* – se ha consolidado como la indiscutible primera potencia en las redes sociales.

Ambas empresas norteamericanas presentan un modelo de negocios basado en la publicidad personalizada, que gira en torno al valor económico de los datos. Nos situamos en el contexto de los mercados de doble cara (*two-sided o multi-sided markets*), que podemos definir como aquellos que reúnen tres requisitos:[7]

- Hay dos demandas diferenciadas, aunque interdependientes entre sí.
- El valor obtenido por uno de los lados de la demanda incrementa a medida que aumenta el número de consumidores de la otra vertiente.
- La existencia de una empresa intermediaria o "plataforma" es necesaria para internalizar las externalidades generadas por uno de los lados de la demanda.

Ello explica que autoridades y expertos en Derecho de competencia se refieran a las plataformas que operan en estos mercados como *gatekeepers* o guardianes de acceso, pues únicamente a través de ellas podrá cada uno de los lados de la demanda acceder al otro lado. Estas plataformas adoptan una peculiar estrategia de precios, subsidiando a uno de los lados de la demanda (el más afectado por el precio) y cargando con los costes al otro lado de la demanda (el que más valora el tamaño de la vertiente opuesta).

Google y *Facebook* se han valido de esta estrategia para maximizar sus beneficios. Ambas han ofrecido sus productos "estrella" a "coste cero" a usuarios de redes sociales y de internet, monetizándolos a través de la venta de espacios de publicidad al otro lado de la demanda. El concepto de "coste cero" o "gratuidad" parece del todo inapropiado para definir la realidad de estos mercados. Es evidente que estas plataformas no prestan sus servicios por filantropía, sino que cobran al consumidor mediante su atención y sus datos.

En efecto, los datos son el activo más preciado de estas plataformas, permitiéndoles ofrecer una publicidad altamente personalizada al consumidor, lo que la hace aún más valiosa a ojos de los publicistas.[8] Asimismo, la existencia de fuertes economías de alcance ha catapultado a estos gigantes hacia otros mercados adyacentes donde los datos ofrecen una significativa ventaja competitiva.[9] Ello les ha permitido constituir amplios ecosistemas compuestos de múltiples servicios que giran en torno a su negocio principal.

---

7 Evans, D. (2002): "The antitrust economics of two-sided markets". *American Enterprise Institute*. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=332022 [consulta: 11/04/2020].

8 Bundeskartellamt (2019): "Bundeskartellamt prohibits Facebook from combining user data from different sources". *Bundeskartellamt.* Disponible en https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html [consulta: 11-04-2021].

9 Crémer, J.; De Montjoye, Y.A. y Schweitzer, H. (2019): *Competition policy for the Digital Era.* Oficina de Publicaciones de la UE. Luxemburgo, pp. 33-35.

En la familia de productos de *Google* se incluyen *Google Search, Android, Chrome, Gmail, Google Drive, Google Maps, Google Photos, Google Play Store* y *YouTube.*[10] Por su parte, *Facebook* integra en su compañía a *Whatsapp* e *Instagram*, entre otras. La combinación de los datos recabados a través de cada uno de estos productos les permitiría elaborar perfiles de usuarios tremendamente precisos e íntimos, que son una de las claves de su modelo de negocios.[11] No obstante, estas actuaciones suelen realizarse sin el conocimiento del usuario concernido, lesionando su derecho de privacidad y protección de datos. Es aquí donde el consentimiento informado desempeñaría un papel crucial.

Por otro lado, los mercados en los que operan ambas plataformas –redes sociales y motores de búsqueda– presentan unos costes de cambio tan elevados que, en ocasiones, llegan al extremo de "encerrar" al usuario, forzándole a permanecer en el servicio ofrecido por la plataforma dominante en contra de sus preferencias. Este es el denominado efecto *lock-in*, que solo podrá ser paliado en la medida en que se reconozca un efectivo derecho a la portabilidad de los datos.

2. La interrelación entre Derecho de protección de datos y Derecho de la competencia

La relevancia de la Protección de datos en el ámbito de la Competencia se explica por la existencia de puntos de conexión entre ambas ramas jurídicas. Esta vinculación parte del carácter dual de los datos:[12]

- **Los datos son un activo esencial (*critical input*) en la economía digital.**

Conviene desmentir el mito según el cual los datos no tienen relevancia desde la perspectiva de la Competencia, pues son ubicuos, no exclusivos y pueden obtenerse a bajo coste.[13] Al contrario, los datos presentan un significativo valor económico, y las empresas invierten infinidad de recursos en construir bases de datos que les proporcionen una ventaja competitiva sobre sus competidores y dificulten aún más su acceso a los mercados.

- **Los datos están inescindiblemente ligados a la dignidad, los derechos fundamentales y libre desarrollo de la personalidad**.[14]

El derecho a la protección de datos surge como una subcategoría del derecho a la privacidad,[15] cuyo objetivo fundamental es garantizar el poder de disposición y

10 Subcommittee on Antitrust (…), *Investigation of Competition… cit*., p. 175.
11 *Ibid*, p. 218.
12 Costa-Cabral, F. Y Lynskey, O. (2017): "Family ties: the intersection between data protection and competition in EU Law". *Common Market Law Review*, 54(1), pp. 11-50.
13 Stucke, M.E/ Grunes, A. P. (2016): *Big Data and Competition Policy*. Oxford University Press. Oxford, p. 8.
14 Costa-Cabral (…), "Family ties:…", *cit.*
15 Alibeigi, A.; Munir, A.B.; Ershadulkarim, M.D y Asemi, A. (2019): "Towards standard information privacy, innovations of the new General Data Protection Regulation". *Library Philosophy and Practice*, 2840, p. 2.

control del ciudadano sobre sus datos personales. La Unión Europea otorga reconocimiento jurídico del máximo nivel a este derecho a través del artículo 8 de la Carta de Derechos Fundamentales de la UE y el artículo 16 del TFUE, donde se dispone expresamente que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan". Su desarrollo en el derecho derivado se remonta a la Directiva 95/46/CE de Protección de Datos, sustituida por el reciente Reglamento (UE) 2016/679 de Protección de Datos de Carácter Personal ("RGPD" o "el Reglamento").

En definitiva, el *big data*, por su doble naturaleza, genera una serie de riesgos que se proyectan sobre sobre distintas áreas del derecho: el Derecho de la competencia, el Derecho del consumo y el Derecho de protección de datos. En lugar de pisarse u obstaculizarse, lo ideal es que estas ramas jurídicas se alimenten mutuamente. En este sentido, la relación entre Protección de datos y Derecho de la Competencia ha de ser bidireccional.

En tanto que la privacidad se ha configurado como una dimensión de la calidad del producto, el Derecho de la competencia puede contribuir a reforzar la Protección de datos.[16] Es evidente que los análisis tradicionales del poder de mercado de una empresa –que se venían fundamentando en la capacidad de comportamiento independiente de una empresa, manifestada en la imposición de precios supracompetitivos– resultan inútiles en un contexto donde los productos se ofrecen al consumidor "gratuitamente". En su lugar, se exige enfatizar en las dimensiones del producto distintas al precio. Particularmente, se ha entendido que la capacidad de explotar y abusar de la privacidad del consumidor sin que su demanda se vea afectada es un indicador de la existencia de poder de mercado.[17] En la UE, la privacidad se ha configurado como un parámetro para medir la calidad del producto utilizado por la Comisión Europea a la hora de valorar operaciones de concentración de empresas tecnológicas, como *Facebook*/*Whatsapp*.[18] Igualmente, en Estados Unidos, la FTC ha reconocido –con motivo de su valoración de la concentración *Google*/*DoubleClick*– el potencial efecto negativo de estas operaciones sobre dimensiones de la competencia distintas al precio, como la privacidad de los consumidores.[19]

La reciente Propuesta de Bruselas de Reglamento de Mercados Digitales[20] realza la capacidad del Derecho de la competencia para complementar a la normativa de Protección de datos, entendiendo que algunas de las obligaciones impuestas a los guardianes de acceso a los mercados digitales incrementarán el nivel de protección ofrecido por el RGPD.[21] Asimismo, el Comité Europeo de Protección de Datos ha solicitado a las autoridades de la competencia que tengan en

16 Subcommittee on Antitrust (…), *Investigation of Competition… cit.*, p. 56.
17 Subcommittee on Antitrust (…), *Investigation of Competition… cit.*, pp. 51-52.
18 Decisión de la CE del 03/10/2014, asunto M.7217 – *Facebook/WhatsApp*, párrafo 87.
19 Decisión de la FTC del 20/12/2007, asunto 071-0170 – *Google/DoubleClick.*
20 Propuesta de Reglamento del Parlamento Europeo y del Consejo *sobre Mercados Disputables y Equitativos en el Sector Digita*l *(Ley de Mercados Digitales)* del 15.12.2020 COM (2020) 842 final.
21 *Ibid*, p. 4.

consideración el impacto de la concentración económica sobre la privacidad, libertad de elección y de expresión de los consumidores.[22]

Por su parte, la Protección de datos puede convertirse en un buen aliado del Derecho de la competencia en diversos sentidos. En primer lugar –y limitándonos al contexto europeo– el RGPD puede ayudar a identificar cuáles son los atributos que integran la privacidad como dimensión de la calidad de un producto.[23] Por un lado, el principio de transparencia se traduciría en obligaciones a cumplir por las empresas en la recogida y uso de los datos. Por otro lado, la responsabilidad proactiva requeriría de las empresas la implementación de medidas de seguridad como la pseudonimización o el cifrado de extremo a extremo, y la puesta en práctica de conceptos como la privacidad desde el diseño o la privacidad por defecto. Estas obligaciones y prohibiciones –castigables con considerables sanciones pecuniarias– [24] modulan las actuaciones de las empresas e impiden ciertos comportamientos con potencial anticompetitivo.

En último término, conviene recordar que el RGPD configura una serie de derechos que refuerzan el control de los individuos sobre sus datos, a efectos de reequilibrar su posición como "contratantes débiles" en los mercados digitales.

3. El Reglamento General de Protección de Datos

El RGPD nace ante las necesidades acuciantes de un entorno caracterizado por la digitalización de la economía y la vida social, donde la vulnerabilidad y exposición a que se ven sometidos los ciudadanos a través de sus datos se hace más patente que nunca. Los escándalos de privacidad invaden los medios día tras día, llegando a sobrepasar los límites de la imaginación humana.[25] Con todo, el *big data* es un ingrediente fundamental de la Inteligencia Artificial, pieza clave del Plan de Recuperación Económica de la UE tras la Pandemia y de su reciente Estrategia Digital.

Este carácter ambivalente del *big data* plantea desafíos impensables en tiempos de la redacción de la Directiva 95/46/CE. El RGPD viene a sustituir a este desfasado instrumento jurídico, atendiendo por vez primera a la Protección de datos desde la óptica del *big data*. El objetivo primordial del Reglamento –en vigor desde el 25 de mayo de 2018– no es otro que conjugar el derecho a la privacidad y la

22 EDPB (2018): "Statement of the EDPB on the data protection impacts of economic concentration". *EDPB*. Disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf [consulta: 17-04-2021].

23 Esayas, S. (2018): "Privacy as a Non-Price Competition Parameter: Theories of Harm in Merger". *University of Oslo Faculty of Law Research Paper*, 2018-26, p.2.

24 Artículo 83.5 del RGPD.

25 Un buen ejemplo es el escándalo de *Cambridge Analytica* destapado en 2018, relacionado con la modulación del voto a las elecciones presidenciales estadounidenses en 2016 de millones de usuarios a través de *Facebook*.

protección de los datos de los individuos con la libre circulación de los datos, para generar una Europa más segura, innovadora y competitiva.

La reforma operada por el Reglamento se fundamenta en dos pilares:

- Por un lado, los principios de transparencia y responsabilidad proactiva, de los que se imbuirán todas las actuaciones de las empresas responsables del tratamiento de datos.
- Por otro lado, el consentimiento informado como piedra angular de un sistema que aboga por el empoderamiento del individuo en lo que a sus datos se refiere. Además, el Reglamento refuerza el control del usuario sobre sus datos carácter personal mediante la creación de nuevos derechos, como son el derecho a la portabilidad de los datos y, en menor medida, el derecho al olvido.

Considerando la naturaleza dual de los datos, estos derechos no solo ofrecen un marco de protección para el individuo, sino que presentan además un importante potencial desde la perspectiva del Derecho de la competencia. Nuestro análisis se centrará en la portabilidad de datos y el consentimiento informado, elementos centrales del RGPD y de particular trascendencia para contrarrestar los abusos de empresas cuyos modelos de negocio se basan en el valor de los datos. Por un lado, estos derechos pueden ser empleados por las autoridades de la competencia como estándares a la hora de valorar la existencia de abusos anticompetitivos.[26] Por otro lado, estos derechos empoderan al individuo frente a las empresas, ayudándoles a tomar decisiones con conocimiento de causa.

4. Categorías de datos

Los datos son bienes heterogéneos, cuyo valor depende del contexto de su utilización, y cuya variedad ha dado lugar a diferentes taxonomías con implicaciones sobre los diferentes agentes económicos.

La primera conclusión que podemos extraer de esta afirmación es que no todas las categorías de datos son relevantes desde la perspectiva de la Protección de datos. Como es lógico, la interrelación entre Protección de datos y Competencia en la UE se producirá exclusivamente en relación con aquellos datos que recaigan en el ámbito material de aplicación del RGPD. En consecuencia, las clasificaciones a que haremos referencia determinarán el alcance de los derechos individuales plasmados en dicho instrumento, la actuación de las autoridades públicas, los derechos de propiedad de las empresas sobre ciertas categorías de datos y la posibilidad de acceder de manera autónoma a los mismos.

A estos efectos, nos valdremos de una doble clasificación de los datos:

- **Según el grado de *identificabilidad*.**

[26] Bundeskartellamt (…), "Bundeskartellamt prohibits Facebook…", *cit.*

A grandes rasgos, podríamos distinguir entre datos anónimos, datos pseudónimos y datos de carácter personal, si bien clasificaciones más pormenorizadas introducen otras categorías intermedias.[27]

El RGPD es de aplicación a los procesos de tratamiento de datos de carácter personal, tal como quedan definidos en el artículo 4.1. Se entiende que son datos de carácter personal "toda información sobre una persona física identificada o identificable".[28]

A *sensu contrario*, el Reglamento excluye a aquellos datos que hayan sido anonimizados; es decir, que pertenecen a individuos no identificables. El GT29[29] ha concluido que cuando una base de datos ha sido completamente anonimizada, el Reglamento no es de aplicación.[30]

La anonimización de datos es por definición un proceso irreversible a través del cual se hace imposible la reidentificación del sujeto. El problema es que los avances de la Inteligencia Artificial han incrementado el riesgo de reidentificación de los usuarios, incluso una vez se han aplicado técnicas de anonimización sobre los datos.

Por ello, hay que distinguir entre dos formas de entender la anonimidad de los datos: anonimización absoluta o anonimización funcional. Mientras que la primera entiende que los datos son anónimos cuando no existe posibilidad alguna de reidentificar a los sujetos, la segunda entiende que existe un riesgo mínimo de reidentificación. Teniendo en cuenta la imposibilidad práctica de aplicar el primer criterio, el GT29 parece adoptar por norma la anonimización funcional.[31] Esto es, se entiende que los responsables del tratamiento han anonimizado los datos cuando el riesgo de reidentificación, sin ser cero, es prácticamente inexistente. No obstante, este proceso es que podría restar tanto valor a los datos como para hacerlos inservibles para el responsable del tratamiento.

Aquí entra en juego el concepto de la pseudonimización. Los datos pseudónimos son definidos como aquellos datos que no pueden atribuirse a una persona sin utilizar información adicional.[32] Las técnicas más frecuentes de pseudonimización de datos son la encriptación, la función hash y la tokenización.[33] A diferencia de la anonimización, la pseudonimización es un proceso reversible;

27 OECD (2019): *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing. París.
28 Artículo 4.1 del RGPD.
29 Grupo de Trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE, de "carácter consultivo e independiente" al que se deben una serie de opiniones y dictámenes que facilitan la interpretación de la derogada Directiva e informan el presente RGPD.
30 GT29 (2014): *Opinion 05/2014 on Anonymisation techniques.* 0829/14/EN WP216.
31 GIL, E. (2015): *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos. España, p. 86.
32 Artículo 4.5 del RGPD.
33 Plath, S. (2016): "And I sit here without identity: faceless. My head aches". *PwC Luxembourg*. Disponible en: https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf [Consulta: 17-2-2020].

existe la posibilidad de reidentificar a los sujetos, siempre que se disponga de la información adicional que permite relacionar al individuo con el dato pseudónimo.

Para analizar si nos encontramos ante datos pseudónimos o ante datos anónimos, el GT29 ha elaborado dos métodos alternativos:

- Realizar un estudio del riesgo de reidentificación.
- Una base de datos será anónima cuando no exista posibilidad de singularizar a un individuo (*singling out*), capacidad de inferir nuevos datos sobre los usuarios (*inference*) o capacidad de asociar datos a un mismo individuo (*linkability*).[34]

El GT29 muestra cierta desconfianza respecto a la eficacia de la anonimización de los datos, concluyendo en su estudio que muchas empresas, pretendiendo crear una base de datos anónimos, obtienen en su lugar datos pseudónimos sometidas a la regulación del Reglamento.

- **Según su procedencia u origen.**

En atención al origen, podemos distinguir entre datos voluntarios, observados, derivados e inferidos.[35] Los primeros encuentran su origen en una acción directa y voluntaria del individual (desde datos posteados, como fotos colgadas en Instagram, hasta registrarse en una página web).[36] Los segundos son obtenidos gracias a la huella que la actividad de un sujeto deja en la red (información captada a través de las *cookies* o la geolocalización) .[37] Los terceros, como su propio nombre indica, derivan mecánicamente de otros datos del sujeto (por ejemplo, cantidad media que el individuo gasta cada vez que compra en una página web).[38] Finalmente, los datos inferidos son el resultado de un proceso analítico basado en la probabilidad.[39] Estos últimos son especialmente conflictivos, e incluyen, por ejemplo, la facilidad para devolver un crédito o el riesgo de desarrollar una enfermedad.

Esta distinción juega un papel importante desde la perspectiva del derecho a la portabilidad de los datos del art. 20 RGPD, tal como ha sido interpretado por el GT29.[40] El art. 20.1 se extiende a los datos que hayan sido "facilitados" por el usuario. El concepto "facilitar" se ha interpretado de manera amplia, para abarcar tanto los datos proporcionados como los datos observados o generados a raíz de la actividad del sujeto.[41] Sin embargo, excluye los datos inferidos y derivados.[42]

---

34 Gil, E. (2015): *Big data, privacidad y protección de datos…cit*., p. 102.

35 Abrams, M. (2014): "The Origins of Personal Data and its Implications for Governance", *The Information Accountability Foundation.*

36 *Ibid*, p. 6.

37 *Ibid*, p. 6.

38 *Ibid*, p. 7.

39 *Ibid*, p. 8.

40 GT29 (2016): *Guidelines on the right to data portability.* 16/EN WP 242 rev.01.

41 *Ibid*, p. 8.

42 *Ibid*, p 8.

5. Las armas del RGPD: consentimiento informado y portabilidad de datos

Hemos afirmado el potencial que presentan ciertas herramientas diseñadas por el RGPD desde la perspectiva del Derecho de la competencia. La cuestión ahora es, ¿Cómo pueden contribuir estas a limitar los abusos de posición dominante en que estarían incurriendo las empresas que controlan grandes bases de datos?

5.1. El consentimiento informado

Antes de entrar en las implicaciones de este instrumento para el Derecho de la competencia, conviene concretar a qué nos estamos refiriendo.

El consentimiento informado es la columna vertebral de un modelo diseñado para proporcionar un mayor control a los individuos sobre sus datos de carácter personal. El RGPD refuerza la importancia del consentimiento del usuario en el escenario de la Protección de datos a la par que incrementa los requisitos exigibles para que dicho consentimiento sea válido. El consentimiento es una de las bases jurídicas –no la única, si bien la más debatida– que justifica el tratamiento de los datos de carácter personal del individuo. El artículo 4.11 del RGPD lo define como una "manifestación de voluntad libre, específica, informada e inequívoca" que implica una "declaración o clara acción afirmativa" por parte del usuario que acepta el tratamiento.

Para considerarse "libre", el consentimiento ha de manifestar una verdadera elección por parte del individuo. Por tanto, la ejecución de un contrato no puede depender del consentimiento del contratante al procesamiento de datos personales no necesitados para dicha ejecución (prohibición de conductas de *tying* o *coupling*).[43]

El consentimiento es informado y específico cuando el usuario conoce cierta información relevante como la identidad del responsable del tratamiento, el tipo de información que será procesada, los fines a los que se destinará dicha información, los derechos de los que goza (como el derecho a retirar su consentimiento en cualquier momento) o los riesgos a los que se enfrenta.[44]

El consentimiento debe otorgarse para cada uno de los fines a los cuales se dirige el tratamiento. Si el tratamiento tiene varios fines, el usuario debe consentir para cada uno de ellos.

El RGPD introduce un nuevo requisito para la validez del consentimiento, y es que este ha de ser "inequívoco"; es decir, no ambiguo. Ello enlaza directamente con la expresa mención a la necesidad de "una declaración o clara acción

43 GDPR-info: "GDPR-consent". *GDPR-info*. Disponible en https://gdpr-info.eu/issues/consent/ [Consulta: 11-04-2021].
44 Véase el artículo 13 RGPD.

afirmativa"[45] por parte del usuario. Sin duda alguna, este es el cambio más significativo de la nueva legislación.

Antes de la entrada en vigor de esta norma, existía un debate acerca de qué forma de manifestación del consentimiento era más adecuada: los sistemas de *opt-in* o los sistemas de *opt-out*.[46] Los sistemas de *opt-in* exigen una acción o consentimiento expreso por parte del usuario cuyos datos personales pretenden tratarse. Por su parte, los sistemas *opt-out* se basan en la presunción del consentimiento, de manera que el usuario ha de manifestar expresamente su negativa al tratamiento de sus datos personales.

El RGPD optó por incluir explícitamente la necesidad de que el usuario manifieste su consentimiento mediante una acción o declaración afirmativa, esto es, mediante un sistema *opt-in*. El Reglamento reconoce que este consentimiento puede manifestarse rellenando una casilla en una página web.[47] Sobre esta premisa, las empresas que operan online han resuelto la prestación del consentimiento a través de las denominadas "políticas de privacidad", que no dejan de ser fuente de numerosas controversias. Y es que el hecho de que implementen sistemas de *opt-in* no quiere decir que el consentimiento prestado sea verdaderamente informado.

Más allá del articulado del RGPD, las autoridades de la competencia europeas han empleado el consentimiento informado para limitar la capacidad de las plataformas digitales de recabar datos de manera indiscriminada. Concretamente, estas han considerado la existencia de un abuso de posición dominante basado en la extensión de la recogida, utilización y combinación de los datos obtenidos a través de distintas fuentes.[48]

La doctrina asentada por la *Bundeskartellamt* en la reciente Decisión de 6 de febrero de 2019 en el Caso *Facebook*,[49] aporta varios elementos relevantes a considerar en la configuración del consentimiento informado desde la perspectiva del Derecho de la competencia. En esta Decisión, la Autoridad alemana examinó la política de privacidad de *Facebook* a la luz del RGPD, para concluir que esta constituía un abuso explotativo incompatible con su Derecho de competencia nacional.[50]

Una importante consideración en su análisis es que el poder de mercado ha de ser tenido en cuenta a la hora de valorar la validez del consentimiento.[51] La existencia de una posición de dominio y la ausencia de alternativas razonables puede viciar el consentimiento dado por los consumidores. En otras palabras, el

45 Considerando 11 del RGPD.
46 GIL, E. (2015): *Big data, privacidad y protección de datos*…*cit*., p. 79.
47 Considerando 32 del RGPD.
48 *Ibid*.
49 Decisión de la *Bundeskartellamt* del 06/02/2019, asunto B6-22/16 – *Facebook*.
50 Bundeskartellamt (2019): "Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing". *Bundeskartellamt*. Disponible en: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4 [consulta: 12-04-2021].
51 *Ibid*.

consentimiento podría no ser verdaderamente "libre" cuando nos encontramos ante modelos de negocio que implican intercambios de datos a cambio de servicios.[52]

Otras autoridades de la competencia en el seno de la UE han llegado a conclusiones coincidentes. Por ejemplo, en una Resolución de 15 de marzo de 2018 relativa a *Facebook* y *Whatsapp*, la AEPD entiende que no existe un verdadero "consentimiento libre, específico e informado"[53] en el sentido del artículo 11 de la LOPD en lo que a sus políticas de privacidad se refiere. La exigencia de dicho consentimiento como prerrequisito para la utilización de un servicio que carece de alternativas razonables "ejerce una influencia real en la libertad de elección del interesado".[54]

En términos similares, la jurisprudencia del Tribunal Constitucional español ha clarificado que, en estos casos, las partes suscriben verdaderos contratos de adhesión,[55] en los cuales el consentimiento del adherente se presta sobre la premisa de "o lo tomas o lo dejas" (*take-it-or-leave-it*). Esta asimetría en la capacidad para fijar los términos y condiciones del contrato es fruto de la posición de dominio disfrutada por *Facebook*.

A consecuencia de lo anterior –y al igual que ciertas cláusulas de estos contratos pueden tenerse por abusivas– "no todo vale" a la hora de redactar estas políticas de privacidad. La *Bundeskartellamt* establece una serie de restricciones a las condiciones de procesamiento de datos de los usuarios.[56] En particular, prohíbe explícitamente la combinación de datos recabados a través del perfil de un usuario de *Facebook* con los datos obtenidos a través de otros productos de la familia de *Facebook* y las páginas web de terceros, salvo que exista un consentimiento voluntario. En consecuencia, el consentimiento no podrá ser un prerrequisito para la utilización del servicio. En otras palabras, la Autoridad alemana impone como remedio una "desagregación interna" de los datos recogidos a través de cada una de las subsidiarias de una empresa que se encuentra en posición dominante.[57]

Cabe decir que este planteamiento ha sido acogido por la Propuesta de Bruselas sobre Reglamento de Mercados Digitales, al prohibir expresamente la combinación de datos procedentes de distintas fuentes, salvo que medie el consentimiento informado de los sujetos concernidos;[58] y exige ofrecer a los usuarios una alternativa menos personalizada en caso de que estos no consientan a tales prácticas.[59]

52 Subcommittee on Antitrust (…), *Investigation of Competition… cit*., p. 79.
53 AEPD (2018): "La AEPD sanciona a WhatsApp y Facebook por ceder y tratar, respectivamente, datos personales sin consentimiento". *AEPD*. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar [consulta: 12-04-2021].
54 *Ibid.*
55 Sentencia de la Sala Segunda del Tribunal Constitucional 27/2020, de 24 de febrero de 2020.
56 Bundeskartellamt (2019): "Case Summary…", *cit*.
57 Crémer, J. (…) *Competition policy for the Digital Era…*, *cit*., p. 80.
58 Artículo 5.a) de la Propuesta.
59 Considerando 36 de la Propuesta.

De ello se derivan consecuencias de distinta índole para operadores y usuarios.

Desde la perspectiva de las plataformas, estas deberán tenerla en cuenta a la hora de diseñar sus políticas de privacidad. A modo ilustrativo, podemos tomar la actualización de la política de privacidad de *Whatsapp* que será plenamente operativa desde el 15 de mayo de este año. Esta reforma plantea permitir la cesión de cierta información recabada a través de *Whatsapp* a *Facebook*, exigiendo a los usuarios a aceptar las condiciones o abandonar el servicio.[60] Evidentemente, los obstáculos impuestos por el RGPD y las autoridades de la competencia europeas impedirían su eficacia en la UE. Consciente de ello, *Whatsapp* ha anunciado que estos cambios no afectarán a los usuarios de la UE.[61]

Aunque establecidos con relación al caso de *Facebook*, idénticas restricciones deberían expandirse a *Google* y su ecosistema de productos. Precisamente, *Google* es, por el momento, el mayor sancionado por infracción del RGPD. En este caso, la CNIL francesa ha impuesto una multa de 50 millones de euros por vulneración de los principios de transparencia y consentimiento informado.[62] Aunque procedente de una autoridad de protección de datos, dicha infracción tiene idéntica significancia para el Derecho de la competencia. A la vista de las circunstancias, *Google* ha propulsado en 2020 una reforma de su política de privacidad destinada a clarificar qué hace con los datos y facilitar la gestión por parte de los usuarios, con el objetivo de cumplir con las exigencias de transparencia y comprensibilidad del art. 5 del RGPD.[63]

Desde la perspectiva de los usuarios, el cumplimiento de estas prescripciones favorece la toma de decisiones conscientes y voluntarias por parte de los consumidores. Ello redunda en beneficios para los competidores, quienes podrán diferenciarse ofreciendo términos de privacidad más favorables que sus rivales más fuertes. Además, la posibilidad de impedir la combinación de datos procedentes de distintas fuentes y optar por una publicidad menos personalizada disminuye la ventaja en término de datos de que gozan las plataformas dominantes frente al resto de operadores del mercado.

---

60 Singh, S. (2021): "WhatsApp to move ahead with controversial "take it or leave it" privacy policy update despite India's strong stand against it". *The Financial Express*. Disponible en: https://www.financialexpress.com/industry/technology/whatsapp-to-move-ahead-with-controversial-take-it-or-leave-it-privacy-policy-update-despite-indias-strong-stand-against-it/2197881/ [consulta: 12-04-2021].

61 The Irish Times (2021): "WhatsApp says European users do not have to share data with Facebook". *The Irish Times*. Disponible en https://www.irishtimes.com/business/technology/whatsapp-says-european-users-do-not-have-to-share-data-with-facebook-1.4452435 [consulta: 12-04-2021].

62 Europa Press (2019): "Francia multa con 50 millones a Google por infringir las normas de protección de datos". *La Vanguardia*. Disponible en: https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html [consulta: 12-04-2021].

63 Lerman, R. (2020): "Google updates terms in plain language after EU scrutiny". *Fortune*. Disponible en: *https://fortune.com/2020/02/20/google-terms-of-service-eu-scrutiny/ [consulta: 12-04-2021]*.

5.2. La portabilidad de los datos

El artículo 20 del RGPD desarrolla este concepto, que puede entenderse como la transmisión de datos de carácter personal de un responsable del tratamiento de los datos a otro, a solicitud del individuo. El interesado tiene derecho a recibir los datos en un "formato estructurado, de uso común y lectura mecánica",[64] así como a la transmisión directa de responsable a responsable, siempre que esto sea posible.

El reconocimiento de un derecho a la portabilidad de los datos presenta connotaciones de primer orden tanto para la Protección de datos como en el Derecho de la competencia, que se manifiestan con especial intensidad en el ámbito de las redes sociales. Por lo que a la primera respecta, este derecho facilita a los usuarios el cambio de una red social a otra. Y es que, cuando los costes de cambio son demasiado altos, el miedo a perder valiosa información personal puede forzar a los individuos a mantenerse en la misma red social en lugar de dar el salto a una alternativa de su preferencia (efecto *lock-in*).

Desde la perspectiva de la Competencia, estos elevados costes de cambio constituyen precisamente una barrera de entrada a los mercados digitales. En un mercado de competencia perfecta, los consumidores deberían tener la posibilidad de transmitir sus datos de carácter personal a voluntad propia. La Comisión Europea ha reconocido que el derecho a la portabilidad de los datos fomentará un mercado más competitivo en el marco de la Unión,[65] al facilitar a las empresas emergentes introducirse en mercados donde gigantes como *Facebook* y los miembros de su familia se encuentran ya consolidados. Como decíamos, estas *start-ups* podrían tratar de atraer nuevos usuarios ofreciendo políticas de privacidad más atractivas.

Desde esta óptica, conductas de *lock-in* en las que incurren ciertos operadores de los mercados digitales podrían constituir una conducta excluyente de la competencia.[66]

Los diferentes enfoques desde los que podría justificarse el derecho a la portabilidad de los datos generan un debate acerca de su naturaleza y alcance. Nos encontramos ante un área a caballo entre el Derecho de la competencia, el Derecho del consumo y la Protección de datos.[67] En la UE, este debate ha quedado desfasado desde el momento en que el RGPD ha tomado la delantera en su regulación.

Aun diseñado en el ámbito de la Protección de datos, este derecho dota a las autoridades de la competencia y a los propios usuarios de otra herramienta a

64 Artículo 20.1 del RGPD.

65 Comisión Europea (2019): "Questions and Answers-General Data Protection Regulation". *Comisión Europea*. Disponible en https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 [Consulta: 16-02-2020].

66 Diker Vanberg, A. y Ünver, M.B. (2017): "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?". *European Journal of Law and Technology*, 8(1), p. 6.

67 2 Kerber, W. (2016): "Digital markets, data, and privacy: competition law, consumer law and data protection". *Journal of Intellectual Property Law & Practice*, 11(11), pp. 856-866.

mayores que pueden emplear para limitar los abusos excluyentes a los que nos veníamos refiriendo.

No obstante, el alcance del derecho a la portabilidad de los datos y su significancia desde la perspectiva de la Competencia dependerá de la interpretación que del mismo se haga.[68]

En este punto, conviene diferenciar varios conceptos cercanos que pueden inducir a la confusión: portabilidad de datos e interoperabilidad en sus diversas especificaciones son distintas caras de una misma realidad, que contribuye en último término a favorecer la complementariedad entre servicios, alentar la multiconexión (*multi-homing*) y proteger al usuario de los efectos inducidos de *lock-in*.

Nos interesan particularmente dos dimensiones de la interoperabilidad. La llamada interoperabilidad de los datos –que también podríamos denominar "portabilidad en tiempo real"– se asemeja a la portabilidad de los datos, si bien exige garantizar un acceso continuo y a tiempo real a la información.[69] En el caso de usuarios profesionales, la interoperabilidad descansaría sobre APIs que permitan el acceso a los datos proporcionados o generados por ellos mismos o por los usuarios finales, requiriendo, cuando sea oportuno, el consentimiento de estos últimos.[70] La interoperabilidad de los protocolos (o interoperabilidad, a secas) permite que dos productos o servicios puedan interconectarse y trabajar juntos a través de medios técnicos.[71] La interoperabilidad es una solución ya consolidada en el Derecho de la competencia, esencial para garantizar una competencia basada en méritos, favorecer la innovación y existencia de servicios complementarios.[72]

Precisamente, la interoperabilidad –o más bien, la falta de ella– fue una de las causas que motivó la apertura de la investigación a *Microsoft* por la Comisión Europea en la primera década del siglo XXI. La Comisión cerró el caso en 2007, exigiendo a *Microsoft*, a modo de remedio, el suministro de la información necesaria a sus competidores para lograr la plena interoperabilidad entre sus respectivos sistemas operativos en el mercado de sistemas operativos para servidores de grupo de trabajo.[73]

Así las cosas, cabría interpretar la portabilidad de datos en sentido restringido, o bien en un sentido más amplio, identificándola con la "portabilidad en tiempo real".

En la práctica, el alcance de este derecho, dotado de un elevado grado de vaguedad e inconcreción en su redacción, no ha sido aún esclarecido. Del tenor

68 Crémer, J. (…) *Competition policy for the Digital Era…*, *cit*., p. 8.
69 *Ibid*, p. 58.
70 *Ibid*, p. 59.
71 *Ibid*, p. 58.
72 *Ibid*, p. 59.
73 Velasco, L.A. y Herrero, C. (2008): "Vinculación y negativa a contratar. Reflexiones en torno al caso Microsoft (sentencia del TPI de 17 de septiembre de 2007)". *Revista de Derecho de la competencia y la distribución*, 2, pp. 193 y ss.

literal del art. 20 podríamos entender que consiste en un derecho a "copiar y pegar" la información suministrada por el usuario que, atendiendo a la interpretación del GT29, abarcaría los datos proporcionados y generados por el usuario.

La Propuesta de Bruselas sobre Mercados Digitales parece imponer mayores cargas sobre aquellos operadores que merezcan la calificación de "guardianes de acceso".

Este instrumento exigiría de dichos operadores una "portabilidad efectiva" que incluya el "acceso continuo y en tiempo real"[74] a los datos proporcionados y generados por estos y la transferencia de los mismos "en tiempo real de forma eficaz, como por ejemplo a través de interfaces de programación de aplicaciones de alta calidad".[75]

El acceso en tiempo real favorece la multiconexión, al permitir a una empresa competidora acceder a toda la información proporcionada a la plataforma dominante por un usuario que simultanea ambos servicios.[76] No obstante, ello obligaría al usuario a mantener una cuenta activa en el servicio ofrecido por la plataforma dominante a efectos de hacer efectiva la portabilidad a tiempo real.[77]

Asimismo, los usuarios profesionales podrán acceder a los datos proporcionados y generados por sus usuarios finales, cuando estos se deriven de la utilización de los servicios ofrecidos por una de estas plataformas digitales.[78]

En definitiva, la Propuesta de Reglamento de Mercados Digitales apuesta por un derecho a la portabilidad de los datos a tiempo real, de mayor calado que el proyectado en el artículo 20 del RGPD. Esta interpretación extensiva quedaría limitada a los supuestos de actuación de un "guardián de acceso", manteniéndose un derecho a la portabilidad más simplificado en caso de que actúe otro operador. Ello es coherente considerando las obligaciones que su implementación implica desde la perspectiva de las empresas. Estas cargas resultarían más gravosas para las empresas que gozan de menos recursos y, en consecuencia, podrían derivar en un efecto dañino sobre la competencia.[79]

Al otro lado del Atlántico, los expertos han lanzado una apuesta aún más contundente, proponiendo garantizar la portabilidad y la interoperabilidad de datos en su máxima expresión.[80] La idea es facilitar la interoperabilidad plena entre redes sociales competidoras y la plataforma dominante, de forma que los usuarios puedan comunicarse a través de distintos servicios, tal como sucede en el ámbito de las telecomunicaciones. Esta medida tendría el efecto inmediato de reducir

74 Artículo 6.1.h) de la Propuesta.

75 Considerando 54 de la Propuesta.

76 Doctorow, C. y Schmon, C. (2020): "The EU's Digital Markets Act: There Is A Lot To Like, but Room for Improvement". *EFF*. Disponible en https://www.eff.org/deeplinks/2020/12/eus-digital-markets-act-there-lot-room-improvement [consulta: 12-04-2021].

77 *Ibid*.

78 Considerando 55 de la Propuesta.

79 Swire, P. y Lagos, Y. (2013): "Why the right to data portability likely reduces consumer welfare: Antitrust and privacy critique". *Maryland Law Rev*, 72(2), pp. 335-380.

80 Subcommittee on Antitrust (…), *Investigation of Competition… cit.*, pp. 386-388.

drásticamente los costes de cambio y, muy especialmente, los efectos de red.[81] De hecho, los verdaderos costes para la empresa dominante no residirían en la implementación de estas medidas, sino en la potencial pérdida de usuarios como consecuencia de la caída de las barreras de entrada.[82]

En cualquier caso, aún tendremos que esperar a la interpretación que de este derecho hagan las autoridades públicas. Lo cierto es que, a día de hoy, no parece que *Facebook* posibilite una verdadera portabilidad de datos, a pesar de sus manifestaciones públicas. Su herramienta para "descargar tu información personal", introducida a la vista de las previsiones del RGPD, es del todo insuficiente para facilitar la migración de datos por parte de sus usuarios.[83]

6. La soberanía del individuo sobre sus datos: ¿Talón de Aquiles del RGPD?

Hasta ahora, hemos enfatizado desde un plano puramente teórico en las posibilidades que los derechos configurados en el marco de la protección de datos ofrecen desde el punto de vista de la Competencia. Las autoridades de la competencia pueden emplearlos como estándares para limitar los abusos anticompetitivos de las empresas. A través de su intervención, refuerzan el control de los individuos sobre sus datos y reequilibran el poder de negociación de estos frente a sus contrapartes.

De esta manera, buena parte de su potencial para favorecer la competencia está en manos de los consumidores y usuarios finales. De nada sirve luchar por un consentimiento verdaderamente informado o por la portabilidad de los datos, si los usuarios consienten ciegamente a los términos impuestos por las plataformas dominantes sin estar dispuestos a explorar siquiera otras posibilidades.

Para aquel que sabe buscar, sí existen ciertas empresas que tratan de diferenciarse de las compañías dominantes a través de términos de privacidad mucho más "amistosos".

En el mercado de los motores de búsqueda, *DuckDuckGo* ha construido una estrategia de negocio focalizada en la privacidad. Su lema no puede ser más claro en cuanto a sus intenciones: "¿Cansado de que te rastreen? Podemos ayudarte. Toma control de tus datos online".[84] "Nuestra política de privacidad es simple: no colectamos o compartimos ninguna información personal tuya".[85] *DuckDuckGo* no recaba información sobre las búsquedas de internet, la dirección IP de los usuarios o

81 Kades, M. y Scott Morton, F. (2020): "Interoperability as a Competition Remedy for Digital Networks". *Washington Center for Equitable Growth*. Disponible en https://equitablegrowth.org/working-papers/interoperability-as-a-competition-remedy-for-digital-networks/ [consulta: 12-04-2021].
82 *Ibid*.
83 Subcommittee on Antitrust (…), *Investigation of Competition… cit*., p. 146.
84 Véase https://duckduckgo.com/?va=b&t=hc
85 *Ibid*.

su historial de búsqueda, desactiva las *cookies* por defecto[86] y su publicidad está exclusivamente basada en el contexto.[87] Con todo, su cuota en el mercado de buscadores de internet en Estados Unidos es inferior al 2,5%.[88]¿Por qué? La realidad es que *DuckDuckGo* ofrece resultados de búsqueda mucho más pobres que *Google*, aunque pretende compensar esta deficiencia a través de su política de privacidad.

Tampoco han faltado alternativas más consideradas con la privacidad de los usuarios en el ámbito de las redes sociales. *Diaspora* o *Ello* son algunos ejemplos de la corriente anti-Facebook que ha ido cobrando fuerza a medida que los escándalos de privacidad protagonizados por esta han agitado los medios. La primera surgió en 2011, como una red social descentralizada, integrada por servidores o *pods* dispersos alrededor del mundo, creados y albergados por los propios usuarios de la red.[89] *Diaspora* asegura no recabar datos para ningún propósito ajeno a permitir la conexión y comunicación entre los usuarios, y permite la interacción entre estos a través de perfiles anónimos.[90] La segunda nació en 2014 como una red social libre de publicidad, con una estrategia *freemium:* ofrece su servicio de forma gratuita, exceptuando ciertas funcionalidades de pago.[91] Actualmente, se define como una red construida por artistas y para artistas.[92]

Aunque ambas siguen en pie, lo cierto es que han fracasado estrepitosamente en su misión de derribar al gigante creado por Mark Zuckerberg. Prueba de ello es que muchos ciudadanos ni siquiera tienen conocimiento de su existencia a día de hoy. Para ser justos, ni siquiera *Google* (con su red social *Google+*) ha sido capaz de desbancar a *Facebook* en su propio juego. La "pegajosidad" de *Facebook* se explica por los efectos de red. ¿Quién va a dejar *Facebook* si el resto de sus contactos no lo hacen?

Es aquí donde entra en juego lo que algunos autores han denominado la "paradoja de la privacidad",[93] la discordancia entre lo que decimos valorar y realmente valoramos nuestra privacidad y nuestros datos. A estas alturas, los consumidores conocen sobradamente los riesgos que para su privacidad entraña el uso de estos servicios y el precio que pagan por ellos. Aun así, deciden adherirse a

86 Duckduckgo: "Privacy". *DuckDuckGo*. Disponible en https://duckduckgo.com/privacy [consulta: 12-04-2021].

87 Esayas, S. (2018): "Privacy as a Non-Price Competition Parameter…", *cit*., p. 9.

88 En marzo de 2021, DuckDuckGo poseía una cuota de mercado del 2,26%. Statcounter (2021): "Search Engine Market Share United States of America". *StatCounter*. Disponible en http://gs.statcounter.com/search-engine-market-share/all/united-states-of-america [consulta: 12-04-2021].

89 Diaspora: "¿Cómo funciona Diaspora?". *Diaspora*. Disponible en https://diasporafoundation.org/about [consulta: 11-04-2021].

90 *Ibid*.

91 Benson, T. (2014): "You Are Not a Product': Ello Wants to Be the Anti-Facebook Social Network". *Vice*. Disponible en https://www.vice.com/en/article/3dkbb3/you-are-not-a-product-ello-wants-to-be-the-anti-facebook-social-network [consulta: 11-04-2021].

92 Véase https://ello.co/

93 Véase, por ejemplo: Williams, M.; Nurse, J. y Creese, S. (2017): "Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things." *15th Annual Conference on Privacy, Security and Trust*, pp. 181-190.

ellos. Precisamente, la escasa atención que los consumidores parecen prestar a su privacidad estimularía la oferta de "servicios gratuitos" que buscan maximizar sus beneficios a través de otras vías. La doctrina habla del denominado "efecto del coste cero",[94] para referirse a la irracionalidad con la que los consumidores adoptan sus decisiones económicas cuando se encuentran ante un producto ofrecido sin ningún coste monetario.

A pesar de las buenas intenciones que sustentan a estas alternativas, su modelo de negocios parece, simplemente, estar abocado al fracaso. El cliente quiere servicios óptimos, gratuitos y sin sobreesfuerzos, y esto es algo que, por el momento, solo empresas como *Google* y *Facebook* están en condiciones de ofrecer.

7. Conclusiones

En los modelos de negocio basados en la publicidad personalizada, el *big data* tiene un valor estratégico, constituyéndose como la fuente de la que emanan la mayor parte de los beneficios que ingresan plataformas digitales como *Google* o *Facebook*.

La doble dimensión del *big data* –cuyos riesgos se proyectan tanto sobre usuarios consumidores como sobre competidores– ha permitido descubrir la utilidad de ciertos instrumentos diseñados desde la óptica de la Protección de datos en el ámbito del Derecho de la competencia. Este es el caso del RGPD, que podría ser (y, de hecho, ha sido) empleado por las autoridades europeas de la competencia como un estándar para concluir la existencia de abusos excluyentes o explotativos, incompatibles con el Derecho de la competencia nacional o europeo.

La actuación de estas autoridades va encaminada a reequilibrar el poder de negociación del consumidor o usuario, como parte débil en los "contratos de adhesión" que suscriben al hacer uso de los servicios ofrecidos por los guardianes de acceso.

El objetivo es que tomen sus decisiones económicas con conocimiento de causa, dejando en sus manos la capacidad de fomentar la competitividad de los mercados. Sin embargo, a la hora de la verdad, el consumidor menosprecia su privacidad frente a la gratuidad o calidad del servicio, la optimización de su tiempo o los inconvenientes de mudarse a una red social donde no están todos tus antiguos contactos.

¿Podría remediarse este defecto concienciando a los usuarios del valor de sus datos, del verdadero precio que están pagando por el uso de los servicios que ofrecen las compañías digitales, haciéndoles ver que existen alternativas disponibles?

En realidad, no parece que la falta de concienciación sea el problema, dado que constantes escándalos de privacidad ametrallan los medios desde hace años.

94 Gal, M.S. y Rubinfeld, D. L. (2016): "The Hidden Costs of Free Goods: Implications for Antitrust Enforcement". *NYU Center for Law, Economics and Organization*, Working Paper No. 14-44.

Todo parece indicar que, en la balanza del consumidor, el peso de la privacidad seguirá siendo muy inferior al de otros intereses en juego.

Y así, los esfuerzos de las autoridades públicas –garantizando la portabilidad de los datos, fomentando políticas de privacidad más claras y transparentes, impidiendo la combinación de datos de diversas fuentes salvo que medie el consentimiento del individuo– habrán sido en balde. Simplemente, la responsabilidad que estas posan sobre el consumidor habitual le viene demasiado grande.