Estudios doctrinales | Civil-mercantil

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

Data power y poder de mercado. Interconexión entre el derecho de la competencia y las normas sobre protección de datos

Nina Polit Sobrino

Graduada en Derecho y Economía.
Universidad Carlos III de Madrid (España)

ninapolit@gmail.com | https://orcid.org/0009-0000-2601-0336

Este trabajo ha sido **finalista** del **Premio Estudios Financieros 2024** en la modalidad de **Derecho Civil y Mercantil**.

El jurado ha estado compuesto por: don José María Blanco Saralegui, don Francisco Javier Arias Varona, don José Luis Blanco Pérez, doña María Medina Alcoz, don Luis Mingo Benedicto, doña Nieves Moralejo Imbernón y doña María José Morillas Jarillo.

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

Extracto

La economía digital ha dado lugar a importantes avances en innovación, pero también ha planteado desafíos en términos de competencia y protección de datos. En mercados digitales, los datos personales se han convertido en uno de los más valiosos activos y en una importante fuente de poder de mercado, otorgando a las plataformas poseedoras una ventaja competitiva única. En años recientes, la jurisprudencia mayoritaria consideraba que cualquier cuestión relacionada con la privacidad y protección de datos no era una cuestión del derecho de la competencia. En contraposición, el objetivo del presente estudio es exponer que ambos regímenes –competencia y privacidad– están profundamente entrelazados porque, por un lado, son las características económicas de estas plataformas digitales las que les permiten recopilar una gran cantidad de datos. Por otro lado, este acceso privilegiado a los datos puede conducir a un mayor afianzamiento de su poder económico a través del aumento de las barreras de entrada, la exclusión de competidores y el desarrollo de estrategias de manipulación informativa. Analizando la reciente doctrina y jurisprudencia, así como las nuevas iniciativas legislativas, se expone que solo mediante la elaboración de una estrategia común y de un enfoque más coordinado entre ambos regímenes, podrá hacerse frente a los desafíos y alcanzar sus respectivos objetivos.

Palabras clave: economía digital; competencia; protección de datos; *data power*; privacidad; poder de mercado.

Recibido: 03-05-2024 / Aceptado: 05-09-2023 / Publicado (en avance *online*): 18-11-2024

Cómo citar: Polit Sobrino, N. (2024). *Data power* y poder de mercado. Interconexión entre el derecho de la competencia y las normas sobre protección de datos. *CEFLegal. Revista Práctica de Derecho*, *287*. https://doi.org/10.51302/ceflegal.2024.22193

Data power and market power. Interconnection between competition law and data protection rules

Nina Polit Sobrino

This paper has been a **finalist** for the **Financial Studies 2024 Award** in the category of **Civil and Commercial Law**.

The jury members were: Mr. José María Blanco Saralegui, Mr. Francisco Javier Arias Varona, Mr. José Luis Blanco Pérez, Mrs. María Medina Alcoz, Mr. Luis Mingo Benedicto, Mrs. Nieves Moralejo Imbernón and Mrs. María José Morillas Jarillo.

The entries are submitted under a pseudonym and the selection process guarantees the anonymity of the authors.

Abstract

The digital economy has led to significant advances in innovation, but it has also raised challenges in terms of competition and data protection. In digital markets, personal data has become one of the most valuable assets and an important source of market power, providing the holding platforms a unique competitive advantage. In recent years, the majority case-law considered that any issue related to privacy and data protection was not, as such, a competition law issue. In contrast, the aim of this study is to show that both regimes –competition and privacy– are deeply intertwined because, on the one hand, it is the economic characteristics of these digital platforms that allow them to collect a large amount of data. On the other hand, this privileged access to data can lead to a further entrenchment of their economic power by raising entry barriers, excluding competitors and carrying out information-manipulation strategies. By analyzing recent doctrine and case-law, as well as new legislative initiatives, it is argued that only through the development of a common strategy and a more coordinated approach between the two regimes can the challenges be met and their respective objectives achieved.

Keywords: digital economy; competition; data protection; data power; privacy; market power.

Received: 03-05-2024 / Accepted: 05-09-2024 / Published (online preview): 18-11-2024

Citation: Polit Sobrino, N. (2024). *Data power* y poder de mercado. Interconexión entre el derecho de la competencia y las normas sobre protección de datos. *CEFLegal. Revista Práctica de Derecho*, *287*. https://doi.org/10.51302/ceflegal.2024.22193

Sumario

«La forma en que reúnes, administras y usas la información determinará si ganas o pierdes»

Bill Gates

1. Introducción

Tradicionalmente las empresas habían competido únicamente en factores como el precio y la calidad de los bienes o servicios. Sin embargo, la llegada del *big data* ha favorecido la innovación y el desarrollo de modelos de negocio disruptivos. Como adelantaba el cofundador de Microsoft, los datos personales se han convertido en objeto de comercio y en uno de los más valiosos activos en la economía digital, constituyendo una importante fuente de poder de mercado[1] y garantizando a las empresas poseedoras el disfrute de una ventaja competitiva única. Si bien potencialmente todas las plataformas digitales pueden controlar y recopilar datos, algunas poseen una capacidad superior para hacerlo. Son estas empresas las que ejercen un verdadero *data power*, lo que plantea una serie de desafíos regulatorios[2]. La recolección, almacenamiento y uso de un elevado volumen[3] de datos por parte de estos gigantes tecnológicos se traduce no solo en el disfrute de una posición privilegiada en el mercado, sino también en la capacidad de influenciar la libre formación de opiniones de sus usuarios.

Por un lado, y en relación con la legislación de competencia, si bien es innegable que las grandes plataformas son el principal motor de la innovación, numerosos expertos doctrinales[4] han señalado que su poder de mercado es tan persistente que se considera improba-

[1] De hecho, en el derecho de competencia alemán, se hace referencia explícitamente a los datos como una fuente de poder de mercado (art. 18(3a) GWB).

[2] El Comité Europeo de Protección de Datos hizo referencia a la potencial acumulación de *poder informacional* por parte de las compañías como parámetro a tener en cuenta a la hora de evaluar los impactos de una concentración.

[3] O las denominadas cinco uves, del inglés: *volume*, *value*, *variety*, *velocity* y *veracity.*

[4] En ese sentido, Schweitzer *et al.* (2018), Crémer *et al.* (2019), Furman *et al.* (2019), ACCC (2019) y Stigler Committee on Digital Platforms (2019).

ble que pueda ser desafiado en un futuro, conllevando múltiples efectos negativos para la competencia, la innovación y la libertad de elección del consumidor[5]. Es principalmente su poder económico y su posición como *gatekeepers* de los servicios de plataforma básicos –en gran medida inevitables– lo que les lleva a disfrutar de numerosas ventajas en el acceso a datos personales. De manera ilustrativa, estas empresas no solo prestan estos servicios de plataforma –que tienden al efecto *winner takes all*– sino que, gracias a la recopilación de datos, construyen ecosistemas digitales complejos, brindando una multiplicidad de servicios vinculados y causando unos elevados costes de cambio (o «jardines amurallados») a los consumidores (OECD, 2020). A través de la oferta de estos servicios básicos cuasi monopolísticos se encuentran a menudo en posición de *gatekeepers* entre los diferentes lados del mercado, lo que les permite recurrir a prácticas desleales y de explotación, tanto frente a usuarios empresariales como a finales (OECD, 2020). De este modo, y en la medida en que las concentraciones o los acuerdos anticompetitivos den lugar a niveles de protección de datos que no sean óptimos, podemos argumentar que la legislación de competencia tiene un papel fundamental que desempeñar (OECD, 2020).

Por otro lado, el control que ejercen las grandes plataformas sobre los datos personales les permite influenciar el comportamiento de los consumidores a través de estrategias de manipulación informativa (OECD, 2020), comportando numerosos peligros para la privacidad de los usuarios y para su derecho a tomar decisiones informadas sobre la recopilación y el uso de sus datos (autodeterminación informativa). Las plataformas en ocasiones ofrecen múltiples servicios por un precio cero (gratis) a los consumidores, que a cambio ceden cantidades ingentes de datos. Aunque esta cesión conlleva numerosos beneficios (en términos de innovación, personalización de los servicios…), también crea nuevos riesgos y posibles perjuicios (discriminación de precios[6], prácticas fraudulentas y manipuladoras…). Sabemos que las empresas responsables del tratamiento de datos están sujetas a la obligación de protegerlos –independientemente de su tamaño o de su posición dominante– y en ese sentido la legislación de protección de datos de la Unión Europea (UE) parte de la idea de que los usuarios tienen el derecho a controlar el uso de sus datos prestando un consentimiento voluntario e informado (art. 6(1) a del Reglamento general de protección de datos, en adelante RGPD)[7]. Sin embargo, en la práctica este mecanismo de *notificación y consentimiento* no funciona eficientemente, al verse los usuarios abrumados por numerosas decisiones –con políticas de privacidad opacas, extensas y de difícil comprensión– y

[5] Para un resumen de los problemas sobre competencia y sus potenciales efectos perjudiciales: capítulo 1 del informe Furman (Furman *et al.*, 2019).

[6] Si bien la evidencia empírica sobre la existencia de precios personalizados es muy reducida y en el análisis de su ilicitud –o ilicitud–, debe considerarse una serie de condicionamientos (Robles Martín-Laborda, 2021).

[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.

por los comportamientos manipuladores a que hemos hecho referencia. Todo ello pone en peligro su soberanía como consumidores y su autodeterminación informativa e impide la correcta protección de su privacidad. Desde un punto de vista económico, aparece un fallo informacional y del comportamiento, que la legislación sobre protección de datos no parece resolver de manera suficiente.

Como podemos observar, ambos problemas –competencia y privacidad– están profundamente entrelazados porque, por un lado, son las características económicas de estas plataformas digitales –con sus tendencias monopolísticas– y la inexistencia de opciones reales para los consumidores[8] las que permiten que los proveedores de estos servicios puedan recopilar una gran cantidad de datos. Por otro lado, este acceso privilegiado (Kerber, 2021) puede conducir a un mayor afianzamiento de su poder a través de (a) el aumento de las barreras de entrada y la exclusión de competidores, y (b) el aprovechamiento de la asimetría de información entre dichas empresas y los consumidores para poner en práctica estrategias de manipulación informativa y conductual (Digital Regulation Project, 2021).

Todo ello nos lleva a la afirmación de que existe una estrecha interrelación y un *vínculo familiar* (Costa-Cabral *et al.*, 2017) entre ambos regímenes. Aunque en el presente estudio nos centraremos en la legislación de competencia, nos cuestionamos si su estrecho objetivo legal centrado en el bienestar y en conceptos de daño basados en precio son capaces de proteger correctamente la competencia en los mercados digitales (Solove, 2013). Así, una de las cuestiones más debatidas por los expertos es si las autoridades deberían tener en cuenta, de manera complementaria, el impacto sobre la privacidad y la protección de datos[9] al evaluar las conductas empresariales en virtud de las normas de competencia (Witt, 2021 y OECD, 2020) –como demuestran los casos de la Bundeskartellamt alemana[10] (en adelante, FCO), con la reciente opinión del abogado general Rantos, y la Federal Trade Commission estadounidense (o FTC) contra Facebook–[11]. Creemos que solo mediante la cooperación efectiva entre autoridades podrán resolverse los importantes desafíos a que se enfrentan las dos legislaciones (Stucke y Grunes, 2016; EDPS, 2014).

---

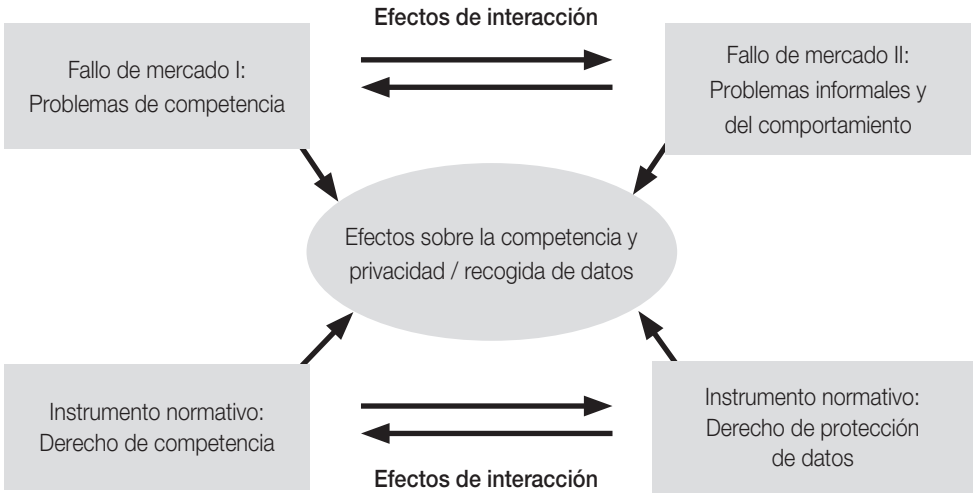
8 En palabras de Robertson (2020): «Los consumidores no suelen tener voz real en cuestiones de privacidad como parte de la calidad de un producto online, ya que normalmente no pueden eludir a los proveedores de servicios digitales predominantes».

9 Ya en 2014, el SEPD argumentó acerca de la importancia de la privacidad y la protección de datos como factores centrales en la evaluación de las actividades empresariales y en su correspondiente impacto en la competitividad, la eficiencia del mercado y el bienestar de los consumidores (EDPS, 2014).

10 Decisión de la Bundeskartellamt de 15 de febrero de 2019 sobre el asunto Facebook, caso B6-22/16.

11 En el mismo sentido se pronunciaron en 2016 la Bundeskartellamt y la Autorité de la Concurrence: «Privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services».

Figura 1. **Efectos de interacción**



Fuente: Elaboración propia a partir de Kerber y Zolna (2022) y Kerber (2021).

De este modo, el presente estudio se encuentra dividido en seis secciones: la sección 1.ª consta de una breve introducción; en la 2.ª se analizará el marco regulatorio relevante; la 3.ª identificará cómo influye el control de datos personales sobre el poder de mercado del que disfrutan las grandes plataformas digitales y discutirá los posibles problemas analíticos en su definición; la 4.ª sección recopilará las posibles conductas anticompetitivas que puedan producirse como resultado del abuso del poder de mercado y se acompañará de una serie de investigaciones[12] sobre las áreas de control de concentraciones y abuso de posición dominante; en la 5.ª se estudiarán los retos a los que se enfrenta la legislación tradicional de competencia y las nuevas iniciativas legislativas que se han desarrollado como respuesta a estos desafíos (Furman *et al.*, 2019), incluyendo la reciente redacción de la sección 19.ª de la Ley de competencia alemana[13] (en adelante, GWB) y, especialmente, la *Digital Markets Act*[14] (en adelante, DMA) a nivel de la UE; finalmente, la sección 6.ª presentará las conclusiones.

[12] Apoyándonos en el estudio de Christophe Carugati (2022), entre otros.

[13] Competition Act in the version published on 26 June 2013 (Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245), as last amended by Article 2 of the Act of 19 July 2022 (Federal Law Gazette I, p. 1214)

[14] Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). PE/17/2022/REV/1. Diario Oficial de la Unión Europea.

2. Marco regulatorio relevante

2.1. Derecho de competencia

El derecho de competencia se aplica a cualquier actividad económica que pueda afectar al comercio entre Estados miembros y persigue una multitud de objetivos, incluyendo la protección de las estructuras de mercado, la libertad económica, el bienestar de los consumidores y el fomento de la eficiencia (EDPS, 2014). Sin embargo, el debate acerca de su objetivo resulta casi tan antiguo como sus propias normas[15]. Durante las últimas décadas, la UE parece encaminarse hacia la consecución del «objetivo de bienestar del consumidor» (o *consumer welfare aim*). De este modo, los fines de las legislaciones sobre protección de datos y competencia parecen converger hacia la protección e impulso del bienestar del individuo, por un lado, y la promoción de un mercado europeo único, por otro. En este contexto, se han llevado a cabo importantes iniciativas legislativas. En relación con las plataformas digitales, cabe destacar el Reglamento (UE) 2019/1150[16], que ha sido complementado por: (a) la nueva regulación *ex ante* de carácter horizontal sobre todos los servicios de intermediación en línea, la *Digital Services Act* (en adelante, DSA)[17], que pretende «modernizar las normas de la Unión en materia de moderación de contenidos y fomentar un entorno en línea transparente y más seguro»; y (b) por la DMA, que regula de manera *ex ante* la actividad de los *gatekeepers* y pretende solventar la incapacidad de la legislación vigente hasta el momento para hacer frente al poder de mercado de las grandes plataformas[18]. Analizaremos su contenido en profundidad en la sección 5.ª.

2.2. Derecho de protección de datos

La base jurídica principal es el RGPD, que regula la forma en que las empresas pueden procesar los datos personales[19] y cuyo régimen está basado en el consentimiento del usuario, que debe prestarse de manera inequívoca, específica, informada y libre. El RGPD

[15] En ese sentido, podríamos destacar las contribuciones de las agencias nacionales de competencia en el marco del Foro Global sobre Competencia de la OECD o las investigaciones de expertos en la materia, como C. D. Ehlermann y I. Laudati (1997), *Objectives of Competition Law*. Hart Publishing.

[16] Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. PE/56/2019/REV/1. Diario Oficial de la Unión Europea.

[17] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). PE/30/2022/REV/1. Diario Oficial de la Unión Europea.

[18] Considerando 5 de la exposición de motivos de la DMA.

[19] Entendidos como cualquier información, adquirida por una empresa, que se refiera a personas físicas y permita su potencial identificación (incluida su ubicación o IP) (art. 4.1 RGPD).

presenta una doble naturaleza: por un lado, los usuarios deben prestar su consentimiento para cualquier tipo de actividad de procesamiento y poseen el derecho a ser informados sobre el modo en que este se va a llevar a cabo; por otro, el responsable del tratamiento está obligado a garantizar que dicho tratamiento se va a realizar en el modo acordado previamente por los usuarios. De esta manera, el RGPD refuerza tanto la protección de los datos personales como la privacidad de los usuarios. En Europa, dado que la protección de datos personales puede ser considerada como un elemento de calidad de un determinado producto o servicio, los acuerdos o intercambios de información entre competidores sobre las políticas de privacidad y el nivel de protección de datos corren el riesgo de caer bajo la legislación sobre competencia –en particular, bajo el artículo 101 TFUE–. De este modo, ciertas empresas podrían encontrarse en una posición dominante en un mercado determinado debido, entre otros factores, a su posesión de datos esenciales que otras empresas necesitarían para poder competir, tal como estudiaremos en secciones posteriores.

3. Control de datos personales y poder de mercado. Problemas analíticos

La privacidad se ha convertido en un tema fundamental a tratar a raíz de la importancia de los datos para poder competir en el marco de la economía digital. Informes de expertos (Cabral *et al.*, 2021), investigaciones de mercado e incluso leyes de competencia como la alemana[20] señalan su importancia como activo estratégico y factor contribuyente al poder de mercado –y por ende, relevante para la competencia–, dada la práctica comercial orientada a obtener una ventaja competitiva basada en el acceso a los mismos (Stucke, 2022).

Sin embargo, las relaciones entre ambos regímenes se producen de maneras diversas y existe una serie de retos analíticos relacionados con la definición del mercado, las barreras de entrada, los factores relacionados con la demanda y la medición del poder de mercado, en general (OECD, 2020). En la presente sección analizaremos dichas cuestiones, haciendo hincapié en cómo puede verse incrementada la posición dominante de las empresas digitales mediante el control de datos de carácter personal.

3.1. Definición del mercado

Se trata del primer paso en el análisis legal de los casos relacionados con acuerdos anticompetitivos, concentraciones y abusos de posición dominante (EDPS, 2014). En general, se considera el mercado de producto –incluyendo productos y servicios con-

[20] 18(3a) German Act against Restraints of Competition (GWB).

siderados sustitutivos–[21], el mercado geográfico y un horizonte temporal –reflejando los cambios en los hábitos de los consumidores y los desarrollos tecnológicos–. El estudio de la OECD (2018) relativo a las herramientas antimonopolio en mercados multilaterales[22] muestra que, dado el número de mercados bilaterales y multilaterales dependientes de los datos de los consumidores, las complejidades relativas a su definición son especialmente relevantes.

En la literatura sobre derecho de la competencia, diversos autores defienden la conveniencia de definir un «mercado de datos». En palabras de Antonio Robles Martín-Laborda (2021), «la existencia de un mercado de datos debería contribuir a la difusión de la información y, en consecuencia, a un mayor bienestar general». Asimismo, Jones Harbour y Koslov (2010) señalaron que «reflejaría la distinción entre una primera recogida de datos y su posterior uso. Las empresas digitales suelen obtener un gran valor de los datos de los usuarios y estos suelen tener importantes consecuencias para la competencia. Por el contrario, las definiciones del mercado de productos basadas *únicamente* en una instantánea del uso actual de datos podrían no captar con precisión este aspecto de la competencia»[23]. No obstante, existen opiniones contrarias como la de Körber (2018), que afirman que no existe un «mercado de datos» sino «un *único* mercado de materias primas».

3.2. Indicadores del poder de mercado

Evaluar el poder de mercado en mercados digitales plantea una serie de retos a las autoridades, no solo a la hora de proporcionar una definición adecuada de este tipo de mercados, sino de cara a examinar la importancia del acceso a los datos personales como una fuente potencial de poder de mercado (OECD, 2022). La legislación de competencia viene reconociendo ampliamente el acceso exclusivo a una materia prima escasa o rara como una fuente de poder de mercado. En mercados digitales, los datos suelen identificarse con esta materia y, por tanto, como un factor contribuyente al poder de mercado[24]. Sin embargo, presentan algunas características que los diferencian de otras materias primas o *inputs* tradicionales, por lo que es necesario tener en cuenta factores como el alcance de los datos

[21] Al determinar el grado de sustituibilidad, la Comisión posee cierta flexibilidad y considera no solo las características del producto y su intención de uso, sino otros factores, como la visión de los competidores, las preferencias de los consumidores y la existencia de diferentes segmentos de estos últimos.

[22] Para un estudio en profundidad, OECD (2018), *Rethinking Antitrust Tools for Multi-Sided Platforms*.

[23] De manera similar, Forrest (2019) ha argumentado que los datos de una empresa y su capacidad algorítmica para analizarlos son en sí mismos productos. De este modo, «la mercantilización potencial de un conjunto de datos funciona como un proxy para definir un universo competitivo».

[24] De hecho, legislaciones como la alemana han sido modificadas para incluir expresamente esta consideración.

considerados[25], la fecha de recopilación y la naturaleza de los flujos de datos, su calidad y precisión (ACCC, 2019) o si se necesita escala[26] u otros recursos específicos[27] para que los datos bajo análisis sean útiles.

3.2.1. Determinante preliminar: cuotas de mercado

La naturaleza estática de las cuotas de mercado se traduce en que solamente funcionan como indicador preliminar de las limitaciones a la sustitución, siendo incapaces de aportar ninguna información sobre el potencial de sustitución de la oferta o de nuevas entradas al mercado (OECD, 2018). Los inconvenientes de las cuotas de mercado son especialmente pronunciados en relación con las plataformas digitales[28], por lo que ofrecen una imagen incompleta como indicadoras de dicho poder. No obstante, la FCO ha indicado que, si bien las cuotas de mercado basadas en los ingresos son menos significativas en mercados dinámicos, la utilización de otras métricas complementarias, como la posesión de una ventaja significativa en la cuota de usuarios cubiertos por una plataforma, podría indicar el potencial de inclinación (*tipping*) del mercado (Bundeskartellamt, 2019). También, en este sentido, la CE en su decisión sobre Google Shopping se centró en las cuotas de mercado por volumen de búsqueda como indicador, dado que constituyen un criterio clave para los anunciantes a la hora de elegir dónde situar sus anuncios. En 2019, la FCO inició investigaciones sobre Amazon[29] y señaló que «en la economía digital, la recopilación de datos representa una actividad que afecta en gran medida a la competencia. El acceso a los datos, sobre todo en el caso de las plataformas y las redes digitales, se ha considerado un factor pertinente para determinar el dominio de mercado».

---

[25] Los datos relevantes en un mercado determinado pueden ser solo un subconjunto de una base de datos mayor, o pueden estar contenidos en múltiples bases de datos diferentes, y la estructura de los datos puede diferir significativamente entre empresas.

[26] Por ejemplo, es probable que el valor marginal de una consulta individual en un motor de búsqueda sea mínimo, ya que el algoritmo necesitará grandes volúmenes de datos para poder mejorar sus predicciones (OECD, Autorité de la Concurrence y Bundeskartellamt, 2016). En cambio, los datos a nivel individual pueden ser especialmente valiosos para productos como las plataformas de redes sociales, en las que el acceso a esos datos es una parte importante del valor de la plataforma (OECD, 2022). Cuando la escala es crucial, o cuando los datos a nivel individual no son portables, los datos podrían contribuir al poder de mercado del operador tradicional.

[27] En ocasiones, para que un conjunto de datos sea útil, puede ser necesario cotejarlo con perfiles de usuarios individuales. Además, es posible que no todas las empresas de un mercado tengan acceso a los conocimientos y recursos necesarios para manejar, procesar y analizar un conjunto de datos.

[28] Por ejemplo, la CE observó en la fusión Facebook/WhatsApp que la frecuente entrada en el mercado y los cortos ciclos de innovación significaban que las altas cuotas de mercado no indicaban necesariamente un mayor poder de mercado.

[29] Decisión de la Bundeskartellamt de 17 de julio de 2019 sobre el asunto Amazon, caso B2-88/18.

3.2.2. Determinante clave: barreras de entrada

Pese a los avances doctrinales y legislativos sigue considerándose que las barreras de entrada son el principal determinante del poder de mercado en plataformas digitales. Autores como Jones Harbour y Koslov (2010) estiman que, dado que existe cierta sustituibilidad entre la evaluación de los impactos sobre la competencia a través de la definición del mercado o de las barreras de entrada, tal vez la última conlleve un enfoque menos controvertido. De este modo, en la presente sección examinaremos bajo qué circunstancias los datos personales pueden ser considerados como tal y, por ende, constituir una fuente de poder económico para las grandes plataformas.

Los mercados intensivos en datos podrían presentar unas barreras de entrada elevadas dada la existencia de rendimientos crecientes de escala, economías de alcance o efectos de red. Los productos digitales requieren importantes costes fijos y costes variables bajos o incluso nulos, ya que incorporar usuarios adicionales puede hacerse sin prácticamente costes. Por tanto, factores como el coste de adquisición de datos (para acceder al mercado relevante e igualar las «ventajas competitivas del primero en llegar») podrían representar importantes barreras y contribuir al poder de mercado de las empresas digitales (OECD, 2022). En defensa de su importancia, diversos organismos de competencia han constatado que el acceso de una empresa incumbente a los datos de los consumidores podría incrementar las barreras de entrada en una serie de mercados de plataforma y permitirle penetrar en mercados adyacentes[30] (ACCC, 2019), tal como determinó la Bundeskartellamt en el asunto Facebook. La expansión vertical de actividad de las empresas en mercados de suministro y distribución supone que estas empresas compiten con los propios comerciantes y creadores de aplicaciones que usan sus plataformas (Hernán Carrillo). Esta expansión vertical aumenta su capacidad para recopilar nuevos datos y les convierte en *gatekeepers* de las tiendas *online* y mercados de aplicaciones de los que son, al mismo tiempo, propietarias y usuarias. Todo ello podría traducirse en comportamientos abusivos y de exclusión de competidores de las plataformas dominantes.

En mayor profundidad, autores como Rubinfeld y Gal (2017) han realizado un análisis de la cadena de valor asociada a los datos personales con el fin de identificar posibles barreras de entrada relacionadas con la recopilación, el almacenamiento, la síntesis y el análisis, y el uso de datos[31]. Con respecto a la recopilación, la Encuesta sobre Plataformas Digitales llevada a

[30] En sentido similar, en la fusión Google/Fitbit, la CE señaló la posibilidad de que los datos de Fitbit reforzaran el dominio de Google en el mercado de la publicidad online, declarando que «ninguno de los competidores de Google tenía acceso a una base de datos o a una capacidad de recopilación de datos equivalente a la de Fitbit y no era probable que adquieran dichos activos sin incurrir en costes significativos» (OECD, 2020).

[31] Por último, con respecto al almacenamiento, la síntesis y el uso de datos, Rubinfeld y Gal (2017) destacan la existencia de posibles barreras de entrada relacionadas con las propias regulaciones legales –las leyes de protección de datos y privacidad–, los acuerdos de exclusividad y los precios o condiciones de acceso

cabo por la ACCC (2019) muestra la importancia de considerar todas las fuentes de datos a las que una empresa tiene acceso, y de determinar si ese acceso es único o replicable[32]. Todo ello determinará si los competidores pueden acceder a los datos necesarios sin incurrir en importantes costes hundidos, lo que en caso contrario significaría que existen importantes barreras.

Además, Rubinfeld y Gal (2017) han observado que pueden surgir importantes barreras tecnológicas a la oferta si las empresas incumbentes logran economías de escala, o *learning by doing*. Los grandes costes fijos y hundidos que conlleva la recopilación de datos a gran velocidad también podrían elevar las barreras de entrada, tal como señalan Pecman, Johnson y Reisler (Pecman *et al.*, 2020). En este sentido, el análisis de la capacidad de un rival para replicar el conjunto de datos de una empresa incumbente en términos de «volumen, velocidad y variedad» de los datos resultaría de vital importancia (OECD, 2020). Asimismo, pueden existir barreras en relación con la demanda cuando están presentes los efectos de red. La existencia de mercados bilaterales y el hecho de que para recopilar ciertos datos sea necesario entrar en un mercado relacionado –lo que Rubinfeld y Gal (2017) denominan «entrada en dos niveles»–, puede incrementar los costes hundidos necesarios para penetrar en el mercado relevante. Por ello, las autoridades han considerado que los efectos de red contribuyen al poder de mercado, y que el impacto de los primeros sobre el segundo se ve intensificado dadas las características de los mercados digitales. En particular, se ha destacado la importancia de los «bucles de retroalimentación positiva» (Tucker, 2018), que pueden observarse tanto en efectos de red directos[33] como indirectos[34] y que, si son lo suficientemente fuertes, pueden llevar a un mercado a inclinarse hacia el monopolio (OECD, 2022), en particular si ningún competidor puede igualar el atractivo de la plataforma[35]. No obstante, la contribución de los efectos de red al poder de mercado es una cuestión controvertida que debe ser analizada dentro de un contexto específico[36] ya que, si bien «conducen

discriminatorios, los costes de cambio elevados (que podrían producir el denominado efecto *lock-in*), los límites a la interoperabilidad de datos y las dificultades para localizar a los consumidores relevantes.

32 En todo caso, y de acuerdo con Maggiolino y Ferrari (2020), «siempre debe llevarse a cabo un análisis empírico de las circunstancias caso por caso para evaluar si los mismos datos (es decir, los datos que responden a las mismas necesidades) podrían obtenerse en otro lugar del mercado». Análisis que, además, debería tener en cuenta el acceso de la empresa tanto a datos propios como de terceros (OECD, 2020).

33 Un aumento en el uso de un servicio digital incrementará su valor, atrayendo así a más usuarios con sus respectivos datos personales y creando un ciclo que se autoperpetúa; un proceso que la ACCC (2019) observó, por ejemplo, con respecto a los motores de búsqueda *online*.

34 Por ejemplo, un crecimiento de usuarios en un lado de la plataforma aumentaría el valor para los anunciantes –que conseguirán más datos de los usuarios–, lo que provocaría nuevas inversiones en la misma y atraería a más consumidores en el lado original, perpetuando así el ciclo (OECD, 2018).

35 Una vez el mercado se ha inclinado a favor de una plataforma, las grandes barreras de entrada dificultan que una nueva empresa pueda competir con la plataforma incumbente, aunque tenga un producto superior y más innovador (Stigler Committee on Digital Platforms, 2019).

36 Calvano y Polo (2021) han sugerido que los efectos de red no solo contribuyen al crecimiento de nuevas empresas, sino que también incentivan una competencia vigorosa para adquirir usuarios, lo que

naturalmente a cuotas de mercado más altas, la presencia de estos efectos por sí mismos no indica necesariamente una falta de competencia» (Bundeskartellamt, 2019). Para determinar su relevancia, deben considerarse factores como las expectativas y preferencias de los usuarios[37] o la existencia de interoperabilidad entre los productos de la competencia.

En opinión contraria, autores como Gilbert y Pepper (2015) relativizan la posesión de datos como una verdadera barrera de entrada, ya que son accesibles económicamente y son bienes no-rivales (pueden obtenerse por otros medios o comprando *sets* de datos)[38], su propiedad está dispersa, tienen poco valor (relativamente) y están sujetos a rendimientos decrecientes. En relación con ello, una cuestión empírica fundamental reside en evaluar el punto en el que se producen las deseconomías de escala y alcance. Por ejemplo, el trabajo de Tucker (2018) sugiere que, al menos para los motores de búsqueda *online*, el acceso a periodos más largos de datos históricos no confiere necesariamente una ventaja significativa. De manera similar, Körber (2016) establece que los datos están sujetos a rendimientos marginales decrecientes, en el sentido de que cada dato adicional produce menos información.

Como vemos, se trata de una cuestión controvertida y cuyo análisis debe realizarse caso por caso, pero cuando se ha determinado que la posesión de datos sí contribuye al poder de mercado, es más probable que este poder se exprese de forma anticompetitiva (Graef *et al.*, 2015; OECD, 2020).

3.3. Comportamiento del consumidor y desequilibrios de poder

La conducta de los consumidores en ocasiones contribuye a la posición de dominio de las grandes plataformas. Por ejemplo, pueden mostrarse reticentes a cambiar de proveedor (ACCC, 2019) aunque sea posible y les beneficie, debido a la costumbre, o debido a una tendencia a no evaluar diferentes opciones de productos cuando actualmente obtienen un producto a precio cero (el denominado *efecto gratuito*, que es relativamente exclusivo de los mercados digitales). Además, suelen ser vulnerables a sesgos como el *framing bias*[39], el *salience bias*[40] y el

conduce a márgenes más bajos. Además, los efectos de red observados en los mercados digitales son diferentes de los de las industrias tradicionales, al no estar conectados a una infraestructura de red específica y, por lo tanto, podrían ser más efímeros como fuente de poder de mercado. En esta línea, Tucker (2018) sostiene que incluso podrían ser una fuente de inestabilidad en estos mercados.

37 En relación con ello, Calvano y Polo (2021) han argumentado que si los usuarios creen que ninguno de sus contactos probará un nuevo servicio, o se resisten a ser los primeros en adoptarlo, incluso los que ofrecen una calidad significativamente mejor podrían tener dificultades para entrar en el mercado.

38 Véase el análisis de la FNE en el caso Uber/Cornershop: https://www.fne.gob.cl/wp-content/uploads/2020/06/aprob57a_F217_2020.pdf

39 O dejarse influir por la forma en que se presentan las diferentes opciones.

40 Implica centrarse en las opciones más destacadas.

default bias[41]. Asimismo, la CE ha identificado la «rigidez» de los consumidores como otro de los factores que contribuye al poder de mercado de estas empresas, amplificando el impacto de ciertas estrategias de los operadores tradicionales, como la preinstalación de aplicaciones en un dispositivo (ACCC, 2019). En el informe Penrose (2021) se destacan las asimetrías de información y los desequilibrios de poder existentes en el sector digital entre consumidores y empresas. Los usuarios de las plataformas *online*, cuyos ingresos proceden de la cesión de sus datos personales a los diversos anunciantes, no pueden tomar decisiones informadas, ya que desconocen el precio real del servicio que se les ofrece, basado en el valor de los datos que estos mismos ceden. Ello puede llevar a que se vean sin más opciones que aceptar las condiciones de recopilación de datos, lo que dificulta la evaluación de la privacidad como una dimensión de la competencia. Dichas asimetrías pueden distorsionar considerablemente el mercado de estos servicios digitales y debilitar la competencia, lo que nos lleva a afirmar que es la combinación de ambos fallos de mercado –desequilibrios de poder y problemas informacionales y del comportamiento– lo que conduce al inmenso poder de las grandes plataformas. Como veremos en la sección 5.ª, lidiar con ellos se convierte en una prioridad fundamental si se quiere hacer frente de manera efectiva a su poder.

4. Conductas potencialmente anticompetitivas

En la presente sección analizaremos tres tipos de conductas potencialmente anticompetitivas –concentraciones, abusos de posición dominante y cárteles y colusión[42]– de acuerdo con los artículos 101 y 102 del TFUE, su posible vinculación con la recopilación excesiva de datos personales por parte de las grandes plataformas y sus efectos perjudiciales sobre la privacidad de los usuarios.

4.1. Concentraciones

Si bien parece aceptarse cada vez más que la privacidad puede ser relevante en las evaluaciones de concentraciones –en la medida en que es una dimensión de calidad que los consumidores valoran y, por tanto, en la que compiten las empresas–, no parece haber ninguna concentración que las autoridades de competencia hayan bloqueado basándose únicamente en estas preocupaciones (OECD, 2020). Debemos tener en cuenta que solo pueden prohibirse las operaciones de concentración susceptibles de obstaculizar de manera significativa la competencia (art. 3 del Reglamento (CE) n.º 139/2004 del Consejo), principalmente mediante la creación o reforzamiento de la empresa resultante. De este modo,

41 Una tendencia a seleccionar la opción por defecto (OECD, 2020).

42 Excluimos del estudio el impacto en las concentraciones, pues no parece haber ninguna concentración que las autoridades hayan bloqueado únicamente por motivos de privacidad.

lo relevante reside en determinar si el acceso a los datos derivado de la concentración refuerza el poder de mercado. Dicho esto, las concentraciones entre empresas que utilizan datos de los consumidores podrían dañar la competencia de dos formas distintas (OECD, 2020): a) reduciendo la calidad de la privacidad y la protección de datos ofrecida en el mercado relevante, o b) elevando las barreras de entrada o los costes de los rivales a través de la combinación de datos de los usuarios.

4.1.1. Detrimento en la calidad de la privacidad y la protección de datos

La CE trata de evitar aquellas concentraciones que priven a los consumidores de ventajas como precios bajos, productos de calidad e innovación, pues estas operaciones incrementan de forma notable el poder de mercado de las empresas[43]. Ello podría producirse si, mediante el acceso a los datos derivado de la concentración, la empresa resultante refuerza su poder y posee capacidad para influir negativamente en las condiciones de privacidad de los usuarios o en otros parámetros de la competencia. Si el poder de mercado en la economía digital puede medirse en función del control de la información personal comercializable, las decisiones sobre concentraciones podrían a su vez tener en cuenta los efectos en el mercado de la combinación de estas capacidades (EDPS, 2014).

Estas preocupaciones son particularmente relevantes en los mercados de precio cero, donde la competencia se basa en gran medida en elementos de calidad y no de precio (OECD, 2018). Algunas concentraciones podrían estar motivadas por el deseo de acceder al conjunto de datos de un competidor, como ocurre en algunas de las denominadas *killer acquisitions* y *nascent acquisitions*. En este sentido, Gilbert y Pepper (2015) sugieren que «la eliminación de un *maverick* que ha desarrollado sistemas innovadores de protección y control de datos podría plantear problemas de competencia al reducir la innovación en la privacidad de los datos, aunque las partes fusionadas no fueran competidoras cercanas». En 2016, la CE permitió la fusión Microsoft/Linkedin[44] y reconoció que la privacidad era un factor de calidad en el mercado de redes sociales, señalando que «las preocupaciones relacionadas con la privacidad no entran en el *ámbito* de la legislación de competencia, pero pueden tenerse en cuenta en la medida en que los consumidores la consideren un factor significativo de calidad y las partes de la fusión compitan entre sí por este factor». Por otro lado, en la fusión Google/DoubleClick[45], siguiendo el precedente establecido por el asunto Asnef-Equifax[46], la CE analizó el modo en que estas empresas utilizaban los datos de los consumidores acudiendo a la legislación sobre protección de datos (y no sobre competen-

[43] Apartado 8.º de las *Directrices sobre la evaluación de las concentraciones horizontales*.

[44] Decisión de la Comisión de 6 de diciembre de 2016 sobre el asunto Microsoft/Linkedin (M.8124).

[45] Decisión de la Comisión de 11 de marzo de 2008 sobre el asunto Google/DoubleClick (M.4731).

[46] Sentencia del Tribunal de Justicia de 23 de noviembre de 2006 sobre el asunto Asnef-Equifax vs. Ausbanc, caso 238/05.

cia) para defender su privacidad y señaló que «independientemente de la aprobación de la fusión, la nueva entidad está obligada en su actividad cotidiana a respetar los derechos fundamentales reconocidos por todos los instrumentos pertinentes a sus usuarios, a saber, entre otros, la intimidad y la protección de datos»[47]. No obstante, las decisiones mencionadas han sido criticadas (Ezrachi y Robertson, 2019) por no tener en consideración el impacto en el rastreo de terceros y por subestimar la ventaja real de los datos agregados. En concreto, argumentaron que la fusión Microsoft/Linkedin «aumentó significativamente el alcance y la variedad de los datos adquiridos a través del rastreo de terceros»[48].

Por otro lado, la CE mantuvo la separación entre las cuestiones relativas a la competencia y las relativas a los datos de los consumidores en su examen de la fusión TomTom/TeleAtlas[49], al no tener en cuenta los impactos sobre la privacidad y la protección de datos personales. Del mismo modo actuaron la FTC estadounidense y la (anterior) Oficina de Defensa de la Competencia inglesa en la posterior fusión Facebook/Instagram (FTC, 2012). Además, en una serie de decisiones posteriores[50], la CE pareció basarse en las leyes europeas de protección de datos para limitar la medida en que las fusiones podrían conducir a una reducción de la privacidad, a través de una mayor recopilación, agregación o uso de los datos de los consumidores.

4.1.2. Elevación de las barreras de entrada o costes

Otra de las maneras en que una concentración puede dañar sensiblemente la competencia es elevando las barreras de entrada[51] a través de la combinación de los datos de los usuarios[52], lo que reforzaría el poder de mercado de la empresa resultante.

---

47 De manera similar, la FTC investigó si esta fusión podría afectar potencialmente a los atributos de la competencia no relacionados con el precio, como la privacidad del consumidor, y la comisaria Pamela Jones Harbour (2007) señaló que podría reducir el nivel de protección de datos ofrecido en el mercado de referencia aunque la legislación de protección de datos ofreciera unos estándares mínimos, ya que la competencia podría elevar los niveles de protección por encima de dichas normas.

48 Por su parte, y sin tener en cuenta los impactos de la combinación de datos de los consumidores en la fusión Google/DoubleClick, la CE «rechazó el impacto a largo plazo sobre el bienestar de millones de usuarios en caso de que la información combinada y generada a través de la búsqueda (Google) y la navegación (DoubleClick) se procesara posteriormente con fines incompatibles».

49 Decisión de la Comisión de 14 de mayo de 2008 sobre el asunto TomTom/TeleAtlas (M.4854)

50 Entre otras, la Decisión de la Comisión de 4 de septiembre de 2012 sobre el asunto Telefónica UK/Vodafone UK/Everything Everywhere (M.6314).

51 United States v. Bazaarvoice (2014), *Competitive Impact Statement*: en 2014, los datos de los consumidores fueron considerados como una barrera de entrada en la fusión Bazaarvoice/PowerReviews, que supuso una concentración horizontal entre dos plataformas de valoración y reseñas, y que no fue permitida finalmente por el Departamento de Justicia de los Estados Unidos.

52 En el asunto Apple/Shazam, la CE reconoció la creciente importancia de los datos personales en los mercados relevantes y observó cómo Apple aprovechaba los datos de sus usuarios para fortalecer el

Condorelli y Padilla (2019) se han referido a una «estrategia de envolvimiento de vinculación de políticas de privacidad», que podría utilizarse para aumentar la cantidad de datos recopilados de los consumidores en el marco de una fusión conglomerada. Bajo esta teoría, una empresa dominante obtendría un amplio consentimiento por parte de sus usuarios, lo que le permitiría utilizarlo en los nuevos mercados en los que se introduzca a través de la fusión y existan consumidores que se solapen en ambos.

En 2014 la CE permitió la fusión Facebook/WhatsApp[53], una fusión entre una red social y una aplicación de comunicaciones, en la que ambas venían recopilando una gran cantidad de datos de los consumidores. Al revisar la fusión, la CE consideró la capacidad de la entidad fusionada para combinar los datos de ambas plataformas y aceptó la alegación por parte de estas de que ello resultaría técnicamente complicado, pero, en cualquier caso, señaló que el impacto competitivo sería limitado dado el importante solapamiento de usuarios (OECD, 2020). En este caso, las consideraciones sobre privacidad también quedaron relegadas a la legislación de protección de datos, afirmándose que «cualquier preocupación relacionada con la privacidad derivada de la mayor concentración de datos en manos de Facebook como resultado de la transacción no entra en el *ámbito* del Derecho de la competencia, sino en el de las normas de protección de datos». Al examinar la fusión, en un primer momento la CE reconoció que la privacidad podría funcionar como un parámetro de competencia no basado en el precio, pero finalmente estableció que la mayoría de las aplicaciones de comunicación de usuarios no competían en privacidad y, por tanto, esta última no era un factor relevante para considerar. Más bien, las diferencias en el nivel de privacidad ofrecido por ambas plataformas fueron utilizadas por la CE para determinar que operaban en mercados distintos (OECD, 2020). Con respecto a esta decisión destaca la crítica de Orla Lynskey (2018), que la tachó de «falacia lógica» al pasar por alto la posibilidad de que WhatsApp se hubiera diferenciado de Facebook con respecto a la protección de datos. Posteriormente en 2017, la CE multó a Facebook por proporcionar información incorrecta o engañosa en el marco de la evaluación de la fusión de 2014[54], pero no se desvió de su anterior decisión, ya que había considerado esta posibilidad al autorizar la fusión.

En los casos en que la combinación de datos tenga el potencial de elevar las barreras de entrada o los costes de los competidores, una posible solución podría ser exigir a la parte fusionada que conceda acceso a su conjunto de datos fusionados (OECD, 2020). En la práctica, varias concentraciones han sido bloqueadas –o autorizadas con condiciones–,

posicionamiento de Shazam en el mercado de la publicidad *online*. Sin embargo, consideró que no obstaculizaría significativamente la competencia, dado que existían mayores agentes de mercado que podrían asimismo competir. En última instancia, consideró que incluso si la entidad fusionada denegara el acceso a los datos de los usuarios de Shazam a los competidores de Apple, sería improbable que ello elevara las barreras de entrada y, por tanto, obstaculizara la competencia.

53 Decisión de la Comisión de 3 de octubre de 2014 sobre el asunto Facebook/WhatsApp (M.7217).

54 En concreto, la CE descubrió que Facebook conocía una posible solución técnica para emparejar automáticamente los perfiles de los usuarios de ambas plataformas digitales.

debido a la preocupación existente acerca de que los datos de los consumidores de la parte fusionada puedan tener un efecto anticompetitivo en el mercado de referencia.

4.2. Abusos de posición dominante

Se trata de conductas de una o varias empresas con posición dominante que restringen u obstaculizan la competencia en los mercados. Como la CE reconoce, el bienestar no viene determinado únicamente por factores relacionados con el precio, sino también por aquellos relacionados con la calidad y la posibilidad de elección del consumidor, preocupaciones que se tornan relevantes tanto para el derecho de protección de datos como para la competencia.

Estas conductas prohibidas vienen establecidas en el artículo 102 del TFUE y en el artículo 2 de la LDC, y la existencia de esta prohibición se condiciona a que la empresa en cuestión disfrute de una posición dominante en el mercado de referencia. Sin embargo, ninguna de las normas nos proporciona una definición del término «abuso», limitándose a establecer una lista *numerus apertus* de conductas abusivas; lo que ha llevado a la CE a calificar los conceptos de posición dominante y explotación abusiva de «indeterminados e inciertos» y a la necesidad de acudir a la jurisprudencia con el fin de lograr una interpretación efectiva. En ese sentido, y en aras de identificar los posibles abusos en mercados digitales, adoptaremos la distinción establecida en el asunto Continental Can[55] entre «abusos de explotación» y «abusos de exclusión», además de contemplar las nuevas formas de abuso surgidas a raíz de las particularidades de estos mercados.

4.2.1. Abusos de exclusión

Podría producirse cuando una empresa dominante restringe el acceso de los competidores a los datos de los usuarios, eliminando o generando desventajas a sus rivales y disminuyendo de manera indirecta el bienestar de los consumidores, que se ven privados de un mercado competitivo eficiente. Además, podría tratarse de asuntos en los que la privacidad desempeña un papel directo en la exclusión de los rivales, como es el caso de Google Privacy Sandbox.

En primer lugar, la banca abierta en el Reino Unido es un buen ejemplo de ello. Tras una investigación sobre la banca minorista en 2016, la Competition and Markets Authority (en adelante, CMA) concluyó que el mercado no funcionaba eficientemente, tras descubrir que existían obstáculos para acceder a la información y barreras para cambiar de banco. La

[55] Sentencia del Tribunal de Justicia de 13 de febrero de 1973 sobre el asunto Europemballage Corporation & Continental Can Company vs. Commission, caso 6/72.

combinación de estas características significaba que había una débil respuesta de los clientes ante las diferencias en los precios o la calidad del servicio, lo que llevaba a los bancos a poseer un poder de mercado unilateral sobre su base de clientes existente (Eversheds Sutherland, 2021). Como resultado, los incentivos de los bancos para competir eran muy bajos y aquellos más grandes y con mayor antigüedad mantenían cuotas de mercado elevadas y estables. Una de las soluciones impuestas por la CMA a los nueve mayores bancos del Reino Unido fue abrir los conjuntos de datos[56] de cuentas bancarias de sus clientes para fomentar la banca abierta (Eversheds Sutherland, 2021). Para abordar los problemas de privacidad, se dio a los consumidores la oportunidad de optar por no compartir sus datos.

Ello guarda relación con la negativa a suministrar[57] y con el concepto de «instalación esencial» (o *essential facility*), entendida como «un producto o servicio que es objetivamente necesario para poder competir eficazmente» y para el que no existe ningún producto o servicio alternativo y en el que los obstáculos técnicos, jurídicos o económicos hacen imposible o irrazonablemente difícil desarrollar una alternativa (Brokelmann, 2006). «Es probable que la negativa a suministrar tal instalación conduzca a la eliminación de la competencia efectiva» o a un perjuicio para el consumidor «cuando los competidores a los que la empresa dominante cierra el mercado se vean impedidos, como consecuencia de la denegación, de introducir bienes o servicios innovadores en el mercado, o cuando sea probable que se ahogue la innovación subsiguiente» (Brokelmann, 2006). Las empresas que han realizado una inversión para controlar datos que les confieren una ventaja competitiva carecen generalmente de incentivos suficientes para permitir a sus competidores (reales o potenciales) el acceso a los mismos, y, como regla general, no tienen obligación de hacerlo ni siquiera en el caso de que ocupen una posición dominante (Robles Martín-Laborda, 2021). La denegación de acceso a tales datos difícilmente constituirá un abuso de dicha posición (Robles Martín-Laborda, 2021). Precisamente por la dificultad de considerar que la negativa de acceso constituya un abuso, esta obligación se ha establecido legislativamente (la PSD2[58] está inspirada en el *open banking* a que hemos hecho referencia). Una medida con alcance más limitado sería posibilitar el ejercicio del derecho a la portabilidad de datos (Robles Martín-Laborda, 2021), al que nos referiremos posteriormente en la sección 5.ª.

[56] De manera similar, tanto las autoridades de competencia francesas como británicas exigieron a las empresas minoristas de energía que pusieran los datos energéticos de sus clientes a disposición de los competidores para preservar la competencia (CMA, 2016 y Autorité de la Concurrence, 2014). Del mismo modo, la autoridad italiana de competencia concluyó que el control exclusivo de las listas de clientes por parte de dos empresas energéticas reguladas podría obstaculizar la competencia en la prestación de servicios energéticos liberalizados (Maggiolino y Ferrari, 2020).

[57] Bajo el espectro del artículo 102 b) del TFUE: «Limitar la producción, el mercado o el desarrollo técnico en perjuicio de los consumidores».

[58] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE.

Finalmente, uno de los casos más relevantes es el de FTC v. Facebook[59], cuya decisión se encuentra pendiente en la actualidad. En él, la FTC por primera vez consideró explícitamente una degradación de la privacidad como una forma relevante de perjuicio al consumidor (Witt, 2021). En diciembre de 2020, la FTC demandó a Facebook por monopolizar el mercado estadounidense de servicios de redes sociales, en violación de la Sec. 2 *Sherman Act*. No obstante, y como veremos más adelante, mientras que la FCO alemana acusó a Facebook de llevar a cabo una conducta de explotación del consumidor, la FTC la calificó como una conducta de exclusión, basándose en teorías del daño distintas. De acuerdo con la FTC, Facebook se había involucrado en dos tipos de conductas excluyentes: por un lado, excluía a los competidores del mercado imponiendo condiciones contractuales anticompetitivas a los desarrolladores de *software* y, por otro, eliminaba la competencia adquiriendo estratégicamente a los competidores (WhatsApp e Instagram). Como señaló la autoridad estadounidense, esta supresión de la competencia causa un perjuicio significativo a los clientes de Facebook, que se ven privados de los beneficios que sí proporcionaría un mercado competitivo, incluyendo una continua innovación, mejoras de calidad y posibilidades de elección. Y según la FTC, esta posibilidad de elección se traduce en que puedan escoger un proveedor de redes sociales que se ajuste más a sus preferencias, relativas a la disponibilidad, calidad y variedad de opciones de protección de la privacidad de datos, así como de su recopilación y uso.

4.2.2. Abusos de explotación

Se refiere a la conducta de una empresa dominante que utiliza su posición de dominio en un mercado concreto para imponer a sus clientes condiciones comerciales injustas que no podría haber conseguido en un mercado competitivo, y que los consumidores no tienen más remedio que aceptar, a falta de alternativas viables. A nivel de la UE, se encuentra explícitamente reconocido en el artículo 102 a) del TFUE.

Una empresa dominante podría abusar de su posición reduciendo el nivel de privacidad y protección de datos que ofrece a los consumidores –como en las investigaciones sobre el intercambio de datos entre Facebook y WhatsApp–, lo que constituye un abuso de explotación en determinadas jurisdicciones. Por ejemplo, Stucke (2018) sostiene que «un monopolista de datos, en la medida en que su modelo de negocio depende de la recolección y explotación de datos personales, puede tener el incentivo de reducir la protección de la privacidad por debajo de los niveles competitivos y recopilar datos personales por encima de estos». En este sentido, autores como Ezrachi y Robertson (2019) han argumentado que en las jurisdicciones que son capaces de perseguir los precios excesivos por parte de las empresas dominantes, las mismas leyes podrían utilizarse para evitar la recopilación injusta de datos por parte de una empresa dominante.

[59] FTC v. Facebook, Case 1:20-cv-03590-JEB.

En la práctica y hasta la fecha, parece existir solamente un caso de explotación en el que se tengan en cuenta la privacidad y la protección de los datos personales. Generalmente, el derecho de competencia de la UE desestima cualquier asunto relacionado con la privacidad y sus infracciones en la evaluación del derecho de competencia. Sin embargo, la Bundeskartellamt señaló que las normas de competencia podían utilizarse para justificar la protección de derechos constitucionales y dictaminó que Facebook había abusado de su poder en el mercado de las redes sociales con respecto a la recopilación de datos desde «fuera de Facebook»[60]. De este modo, esta decisión es la primera que ha establecido una teoría del daño relativa a una reducción de la privacidad como un abuso de posición dominante y, en ella, la FCO tuvo que lidiar con importantes obstáculos jurídicos; a saber: (a) probar que los términos de recopilación de datos de Facebook eran injustos y (b) establecer una relación de causalidad entre la ausencia de competencia y el daño causado por Facebook en aras de poder aplicar el derecho de competencia. Al evaluar las prácticas de Facebook en relación con la recopilación de datos, la Bundeskartellamt mantuvo un contacto regular con las autoridades de protección de datos y determinó que estas eran incompatibles con las normas del RGPD, lo que equivalía a un abuso de posición dominante. En dicha evaluación adoptó un enfoque acumulativo, indicando que la sola infracción del RGPD podría no equivaler a un daño competitivo en sí mismo, pero que era relevante desde la perspectiva del derecho de competencia y estableció que el abuso de la posición de mercado de Facebook podría incorporar elementos de esta infracción (Witt, 2021). Argumentó que su poder de mercado ponía esencialmente a los consumidores en una posición de «lo tomas o lo dejas» y concluyó que sus prácticas contribuían a afianzar su posición dominante (Bundeskartellamt, 2019). De este modo, dedujo la relación causal entre la posición dominante y el perjuicio, del hecho de que el desequilibrio de poder entre Facebook y sus usuarios era un factor clave que contribuía a la ilegalidad de la conducta de Facebook en virtud del RGPD. La FCO se refirió a ello como una «causalidad normativa» y consideró que no era necesario establecer una hipótesis de contraste para demostrar que Facebook no habría podido imponer estas condiciones de recopilación de datos a los consumidores en un mercado competitivo (Witt, 2021). Como remedio, obligó a Facebook a modificar sus prácticas de recogida y tratamiento de datos en un plazo de 12 meses. Facebook recurrió la decisión ante el Tribunal Regional Superior de Düsseldorf, que suspendió la orden en agosto de 2019[61]. En particular, no aceptó que una posible violación de las normas de privacidad desencadenara automáticamente una violación de las normas antimonopolio en el caso de una empresa dominante[62]. La suspen-

60 Decisión de la Bundeskartellamt de 15 de febrero de 2019 sobre el asunto Facebook, caso B6-22/16.

61 Decisión del Tribunal Regional Superior de Düsseldorf de 26 de agosto de 2019 sobre el asunto Facebook/Bundeskartellamt, caso Vi-Kart 1/19 (V).

62 Además, argumentó que los usuarios decidían de forma autónoma si estaban de acuerdo con los términos y condiciones de Facebook cuando se registraban en el servicio, y consideró que la recopilación de datos por parte de Facebook no constituía una explotación, ya que los consumidores podían seguir poniendo los mismos datos a disposición de otras empresas (Witt, 2021).

sión de la orden eximió a Facebook de aplicar la anterior decisión de la Bundeskartellamt. Posteriormente, el Tribunal Federal de Justicia consideró que Facebook había incurrido en una conducta anticompetitiva y anuló la orden del Tribunal Regional. Aunque no rechazó el concepto de perjuicio de la FCO puramente basado en la privacidad, el Tribunal Federal argumentó que Facebook había perjudicado a los consumidores al aprovechar su posición de dominio para privarles de una opción que un mercado competitivo les habría ofrecido (Witt, 2021). El tribunal de Düsseldorf decidió suspender el procedimiento y plantear una cuestión prejudicial al TJUE[63], cuestionándole si una autoridad nacional de competencia puede aplicar el RGPD como base para una decisión sancionadora en virtud del derecho de la competencia (Witt, 2021). En este contexto, en el dictamen publicado en septiembre de 2022 ante el TJUE, el abogado general Rantos validó el enfoque de la autoridad alemana que, finalmente considerado por el tribunal[64], ha supuesto un cambio de extrema importancia en la jurisprudencia[65], con relevantes implicaciones en lo que a la cooperación entre autoridades de competencia y de protección de datos se refiere. Analizaremos esta cuestión en mayor profundidad en la sección 5.ª.

4.3. Cárteles y colusión

Las prácticas de colusión que acuerdan el nivel de privacidad ofrecido a los consumidores podrían constituir una infracción del derecho de la competencia, al igual que cualquier otro acuerdo sobre calidad, producción o precio. Sin embargo, no está tan claro que el intercambio de datos facilite dichas prácticas colusorias si los datos no incluyen información sobre precios, calidad, innovación o elección[66]. De hecho, en la práctica se ha tendido a permitir el flujo de datos personales, ya que normalmente se considera que fomenta la competencia (OECD, 2020). Además, características como el dinamismo, la utilización de diversas plataformas simultáneamente (*multi-homing*), la diferenciación y complementariedad de productos o la constante innovación en mercados digitales dificultan el consenso sobre los términos

63 Desafortunadamente, la cuestión prejudicial no incluye una pregunta acerca del concepto de daño en términos del artículo 102 del TFUE, ya que la FCO (no estando segura de cuál era la interpretación correcta) había decidido no aplicar el artículo, además de la prohibición alemana del abuso de posición dominante. Si el artículo 102 a) del TFUE cubriera los casos de explotación consistentes en la recopilación excesiva de datos, la FCO habría tenido la obligación legal de aplicar el mencionado artículo, además de la prohibición alemana de abuso de posición dominante, y habría infringido la legislación de la UE al no hacerlo. La obligación de aplicar el artículo 102 de la TFUE, además de la legislación nacional sobre competencia en los casos contemplados por el mismo, se desprende del Reglamento (CE) n.º 1/2003 del Consejo, de 16 de diciembre de 2002.

64 STJUE, de 4 de julio de 2023, Asunto C-252/21 (Meta Platforms Inc).

65 Hasta ahora apoyada mayoritariamente en el caso Asnef-Equifax.

66 Debemos tener en cuenta que los datos generalmente no constituyen información estratégica –como sí lo son los precios o las cantidades futuras–, por lo que su intercambio difícilmente favorecerá la colusión.

del acuerdo colusorio[67] e incluso su posterior viabilidad. El estudio de Christophe Carugati (2022) muestra que los diferentes países investigan la privacidad en los casos antimonopolio y de control de concentraciones, pero no en los de cártel. El asunto Asnef-Equifax[68] es citado a menudo como uno de los primeros casos en que el TJUE examinó cuestiones de privacidad (si bien el riesgo que señalaba el tribunal era de exclusión). No obstante, en última instancia se remitió a la legislación sobre protección de datos, en lugar de a la legislación sobre competencia. Al considerar el acuerdo que facilitaba el intercambio de datos personales, el tribunal señaló: «Los posibles problemas relativos a la sensibilidad de los datos personales no son, como tal, una cuestión del derecho de la competencia, sino que pueden resolverse sobre la base de las disposiciones relativas al derecho de protección de datos».

5. Posibles remedios

Durante mucho tiempo, y como hemos observado a lo largo del presente estudio, las legislaciones sobre competencia y protección de datos se han considerado separadas, con objetivos diferentes y con la tarea de hacer frente a distintos fallos de mercado. Esta es la razón por la que el caso Facebook de la FCO ha sido tan controvertido[69], al tener en cuenta los problemas de privacidad en un caso de competencia y vincularlo directamente con el derecho de protección de datos (Kerber, 2021). El debate sobre el inmenso poder económico de las grandes plataformas ha llevado a la conclusión de que existen múltiples interdependencias y que, por lo tanto, un enfoque de separación pura ya no es una estrategia adecuada (Kerber, 2021). Si ambas leyes se aplican independientemente, podrían surgir tres problemas[70]: conflictos[71], lagunas[72] e infraexplotación de sinergias[73]. Para lidiar con ellos, podrían emplearse

67 En ese sentido: M.7217 - Facebook/WhatsApp.

68 Sentencia del Tribunal de Justicia de 23 de noviembre de 2006 sobre el asunto Asnef-Equifax vs. Ausbanc, caso 238/05.

69 Por lo tanto, no es sorprendente que la principal crítica a la decisión de la FCO proceda del enfoque tradicional (mantenido asimismo por la Comisión en la mayoría de los asuntos) de que estos dos regímenes jurídicos deben mantenerse distantes.

70 Expuestos por Kerber (2021).

71 Como sería el caso si los remedios del derecho de competencia obligaran al intercambio de datos personales, con sus potenciales efectos negativos para la privacidad; o si las autoridades de ambos regímenes emitieran decisiones contradictorias o incompatibles entre sí (Kerber, 2021).

72 Podrían existir casos en los que una conducta con efectos negativos para la competencia o la privacidad no sea abordada por ninguno de los regímenes, al considerar que está fuera de sus competencias. Además, también podrían darse estas lagunas si alguna de las leyes se aplica insuficientemente. El caso alemán Facebook podría servir como ejemplo, ya que, en un primer momento, la legislación de protección de datos de la UE no aplicó el RGPD y fue la FCO la autoridad que posteriormente intervino para solventar esta laguna.

73 En este sentido, véase Graef *et al.* 2018. Especialmente importantes son los casos en que la aplicación de ambas leyes va en una misma dirección, apoyando tanto la competencia como la privacidad.

dos estrategias regulatorias básicas (Kerbet, 2021): estrategias unilaterales y estrategias de cooperación. Analizaremos ambas a continuación.

5.1. Estrategias unilaterales

Existe un amplio consenso acerca de la necesidad de que cada una de las legislaciones tenga en cuenta de manera unilateral estos efectos de interacción.

5.1.1. Derecho de competencia tradicional

El caso alemán Facebook ha generado un debate sobre cómo integrar las preocupaciones de privacidad en el marco del derecho de competencia (OECD, 2020, pp. 24-41) para lograr una conciliación efectiva entre ambos regímenes[74]. Si bien es una estrategia unilateral y no analiza directamente la interacción entre ambos regímenes, constituye un gran paso hacia delante.

A pesar de la proliferación de nuevos instrumentos legislativos (como la DMA o la Sec. 19.ª GWB) tendentes a combatir el poder económico de las grandes plataformas, su utilidad reside en complementar (y no sustituir) al derecho de competencia tradicional (Kerber, 2021)[75]. En este sentido, la 10.ª enmienda del derecho alemán de competencia no solo ha incorporado la nueva Sec. 19.ª GWB, sino que ha introducido una serie de reformas con el fin de proteger la competencia en la economía digital. A diferencia del informe Furman o de la DMA, estas reformas se han incorporado directamente en el derecho de competencia y serán aplicadas por sus autoridades[76]. Especialmente innovador es el concepto utilizado para determinar qué empresas están sujetas a estas nuevas normas: aquellas con una

Por tanto, cabe preguntarse qué soluciones regulatorias pueden contribuir a mejorar estas sinergias o a crear nuevas vías para que las legislaciones se ayuden mutuamente a alcanzar sus objetivos (Kerber, 2021).

74 Dado que los daños sobre la privacidad también pueden considerarse en cierta medida como perjuicios a los consumidores dentro del derecho de la competencia, y teniendo en cuenta que determinadas estrategias de recopilación de datos por parte de las grandes plataformas tienden a elevar las barreras de entrada y a provocar efectos de exclusión, existen posibilidades teóricas para tener en cuenta los efectos de la privacidad (OECD, 2020).

75 Especialmente con respecto al control *ex post* del comportamiento abusivo de las empresas dominantes (art. 102 TFUE). La aplicación de este último sigue siendo absolutamente relevante, ya que los primeros olvidan perseguir determinadas conductas, como los acuerdos anticompetitivos y, más relevante si cabe, las concentraciones.

76 Siguiendo las previsiones de la nueva Sec. 19a GWB, la FCO inició en 2021 diversas investigaciones contra Facebook, Amazon, Google y Apple.

«importancia capital para la competencia en los mercados»[77]. Una vez que la empresa se sujeta a estas normas, la autoridad de competencia puede prohibirle una serie de comportamientos[78] que en gran medida coinciden con los previstos en la DMA, pero cuya redacción es mucho más abierta (Kerber 2021). A diferencia de la DMA, estos comportamientos no están directamente prohibidos[79], sino que se ofrece a la autoridad alemana una lista de opciones sobre las conductas que puede prohibir (Kerber y Specht-Riemenschneider, 2021). Además, dado que la intención de la enmienda es lograr una aplicación rápida y eficaz, se introduce un desplazamiento de la carga probatoria, lo que implica una presunción de que tales comportamientos dificultan la competencia, aunque las empresas tienen la posibilidad de justificarlos (Kerber, 2021). Por último, mencionar que algunos de los comportamientos prohibidos también hacen referencia a los intereses de los consumidores con respecto a sus datos personales[80] (Witt, 2021).

A pesar de ser considerado un mecanismo innovador y un complemento valioso para la DMA (Witt, 2021), los expertos han cuestionado su eficacia. El derecho de competencia tradicional no puede resolver eficazmente los problemas de privacidad debido a su limitación para abordar los fallos de mercado informacionales y del comportamiento, cruciales en el contexto del poder económico de las grandes plataformas digitales (Kerber, 2021).

5.1.2. DMA

La constitución de un mercado único digital (DSM) constituye una prioridad fundamental para la UE, que recientemente ha promulgado la DSA[81] y la DMA[82], basadas en el Reglamen-

---

77 O como la Sec. 19a (1) GWB reza: *paramount significance for competition across markets.* Esta definición enfatiza el carácter conglomerado de las grandes plataformas digitales, la existencia de ecosistemas y los efectos interconectados entre mercados, ampliando así la consideración del poder económico de estas compañías más allá de los conceptos tradicionales de dominio de mercado centrados en mercados específicos (Kerber y Specht- Riemenschneider, 2021).

78 *Self-preferencing*, el uso de los datos recopilados para elevar las barreras de entrada, el impedimento de la interoperabilidad o la portabilidad de datos.

79 En ese sentido, Franck/Peitz.

80 En particular, la Sec. 19a (2) n.º 2, 3, 4 y 5 GWB se centra en diferentes aspectos de la protección de la libertad de elección de los usuarios (incluyendo la interoperabilidad y la portabilidad de datos); y la n.º 4, que prohíbe a estas grandes empresas procesar datos de otros servicios sin el consentimiento del usuario, se asemeja en gran medida a la obligación del artículo 5(a) DMA (y, por tanto, a los remedios utilizados en el caso alemán Facebook).

81 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). PE/30/2022/REV/1. Diario Oficial de la Unión Europea.

82 Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE)

to (UE) 2019/1150[83]. Hemos decidido incluir un apartado específico para la DMA, debido a que tanto sus objetivos –disputabilidad y equidad–[84] como su estructura –regulación *ex ante* de conductas prohibidas *per se* y previsión de un mecanismo de actualización para adaptarse al dinamismo de los mercados digitales–[85] difieren considerablemente de aquellas del derecho de competencia tradicional[86]. Además, y como veremos a continuación, tampoco la designación de *gatekeepers* requiere la definición de mercados o una evaluación de la posición dominante en un mercado determinado –evitándose los problemas que hemos mencionado más arriba–

A diferencia de iniciativas como el informe Furman o la nueva Sec. 19.ª GWB, la DMA no se encarga de una manera directa de las grandes firmas digitales, sino que pretende hacer frente al dominio de las grandes plataformas *online* consideradas como *gatekeepers*[87]. Por otro lado, dado que el tradicional control *ex post* resulta lento e inefectivo, la estrategia regulatoria básica de este instrumento se centra en que las plataformas tengan que cumplir directamente con las obligaciones previstas, sin la necesidad de investigaciones, prueba del daño o decisiones de la Comisión[88], lo que ofrece la oportunidad de que estas normas se apliquen de manera mucho más rápida (Kerber, 2021).

2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). PE/17/2022/REV/1. Diario Oficial de la Unión Europea.

83 Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. PE/56/2019/REV/1. Diario Oficial de la Unión Europea.

84 Considerando 7.º DMA.

85 Artículos 12 y 19 DMA.

86 En el considerando 11.º DMA se establece de manera explícita que este instrumento persigue intereses complementarios, pero distintos, a los del derecho de competencia tradicional (arts. 101 y 102 TFUE).

87 El artículo 3(1) DMA designa como tal a aquellas empresas que: a) tengan una gran influencia en el mercado interior; b) presten un servicio básico de plataforma que sea una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales; y c) tengan una posición afianzada y duradera, por lo que respecta a sus operaciones, o es previsible que alcancen dicha posición en un futuro próximo. El artículo 2(2) DMA define diez servicios básicos de plataforma, entre los que se encuentran los servicios de intermediación en línea (como el *marketplace* de Amazon), los motores de búsqueda *online* (como el de Google) y los servicios de redes sociales *online* (como Facebook). Además, para facilitar su designación, la norma utiliza umbrales cuantitativos concretos (art. 3(2) DMA), con respecto al volumen de negocios, el número de empresas y usuarios finales, etc., cuyo cumplimiento conduce a una fuerte presunción acerca de la naturaleza de dicho proveedor como *gatekeeper*. Sin embargo, esta presunción puede refutarse por las empresas (art. 3(5) DMA), y la CE puede designar a una empresa como guardián tras realizar una investigación de mercado, si no se cumplen estos umbrales cuantitativos (art. 3(3) DMA).

88 La DMA distingue entre las obligaciones del artículo 5 y del artículo 6. Mientras que las obligaciones del artículo 6 podrían necesitar una mayor especificación, las obligaciones del artículo 5 se suponen lo suficientemente claras como para que los guardianes puedan cumplirlas directamente. En la medida en que sea necesaria una mayor especificación, la DMA ofrece un procedimiento que incluye la posibilidad de un diálogo regulador entre la Comisión y los guardianes.

En relación con los objetivos de la DMA, y más concretamente, con el de equidad (Kerbet, 2021), el reglamento observa una relación directa entre la posición de *gatekeeper* y los «graves desequilibrios en el poder de negociación», que conducen a «condiciones injustas tanto para los usuarios profesionales como finales de los servicios básicos de plataforma en detrimento de los precios, la calidad y la innovación» (considerando 4.º DMA). Estas prácticas desleales podrían causar efectos negativos, como un reparto injusto del excedente, en el que ni empresas ni usuarios finales disfrutarían de las justas recompensas por sus contribuciones al bienestar económico y social (Digital Regulation Project, 2021). Ello guarda relación con los clásicos abusos de explotación por parte de empresas con poder de mercado, regulados en el derecho tradicional de competencia (Schweitzer, 2021); lo que significaría que este concepto de equidad podría lidiar con ambos fallos de mercado (desequilibrios de poder, por un lado, y problemas informacionales y del comportamiento, por otro) y proteger a los usuarios empresariales frente a las normas opacas de las plataformas, las restricciones indebidas a su capacidad para competir y la privación de las recompensas por sus resultados (Kerber, 2021).

Por otro lado, la DMA merece un análisis de sus efectos sobre la privacidad y la protección de datos (Kerber, 2021). El considerando 35.º DMA enfatiza la necesidad de las obligaciones «para abordar las preocupaciones de orden público identificadas», mencionando explícitamente la «necesidad de proteger la intimidad y combatir las prácticas comerciales engañosas». De esta manera, en lo que respecta a los usuarios finales, esta interpretación permite tener en cuenta los objetivos de la legislación de protección de datos, a saber, la autodeterminación informativa/soberanía del consumidor con sus dimensiones de (a) fortalecimiento de la autonomía (y garantía de elección), y (b) protección contra la manipulación informativa y del comportamiento (poder de información) (Kerber y Specht-Riemenschneider, 2021). En relación con la dimensión a) y de acuerdo con la solución establecida en el caso alemán Facebook, la regulación asimétrica del artículo 5(2) DMA obliga a los guardianes a recabar un consentimiento adicional para la combinación de datos personales procedentes de distintas fuentes, cuya justificación se incluye en el considerando 36.º de la misma norma[89]. Sin embargo, esta solución ha recibido numerosas críticas, en el sentido de que los consumidores pueden tener los inconvenientes habituales (como en el RGPD) a la hora de prestar un consentimiento libre e informado (Kerber, 2021) y pueden verse empujados (*nudged*) a prestar su consentimiento en favor de las plataformas a través de los diseños manipuladores de las arquitecturas de elección (*dark pattern*

[89] Considerando 36.º DMA: «El tratamiento de datos personales […] proporciona a los guardianes ventajas potenciales en términos de acumulación de datos, lo que crea obstáculos a la entrada al mercado [...]. Para garantizar que los guardianes no menoscaben deslealmente la disputabilidad de los servicios básicos de plataforma, dichos guardianes deben permitir que los usuarios finales puedan elegir libremente participar en tales prácticas […] ofreciéndoles una alternativa menos personalizada, aunque equivalente, y sin condicionar el uso del servicio básico de plataforma o de determinadas funcionalidades de este al consentimiento del usuario final»

behavior). Si bien la CE trata de evitarlo –como se observa en el considerando 37.º[90]-, no parece ser suficiente, por lo que se han propuesto medidas adicionales, como la inclusión de disposiciones complementarias[91] o incluso la prohibición absoluta del tratamiento de datos personales, si se considera que es especialmente peligroso[92]. Esta última solución también tendría sentido para alcanzar el objetivo de disputabilidad, ya que si la mayoría de usuarios prestaran su consentimiento, las grandes plataformas seguirían disfrutando de importantes ventajas competitivas (Kerber y Zolna, 2022). Más allá del artículo 5(2) DMA, existen una serie de disposiciones –arts. 5(3), (5), 6(3) y (4)– que pretenden fortalecer la capacidad de elección tanto de empresas como de usuarios finales y que al mismo tiempo funcionan como instrumentos para afianzar la disputabilidad y la competencia en los mercados digitales[93] (Kerber, 2021). De nuevo, y de acuerdo con el informe Furman, no queda claro si dichas obligaciones pueden aplicarse de manera eficaz tal como están especificadas o si resulta necesaria una autoridad reguladora con amplios conocimientos tecnológicos (Kerber, 2021).

Por otro lado, dado que los artículos 6(2), (10) y (9) guardan una estrecha relación entre sí, merecen ser analizados de forma conjunta. Si bien los considerandos parecen sugerir que su principal justificación es afianzar la competencia y la disputabilidad, la lectura de los artículos deja entrever cuestiones de equidad (Kerber, 2021). El hecho de que el proveedor de una plataforma se encuentre técnicamente en una posición única para observar todo lo que ocurre en ella y, por tanto, pueda recopilar todos los datos generados por las interacciones entre empresas y usuarios finales en la misma, conduce a una posición de control exclusivo sobre estos datos por parte del *gatekeeper* (Kerber y Zolna, 2022). Sin embargo,

---

90 Considerando 37.º DMA: «Cuando el guardián de acceso solicite el consentimiento, debe presentar proactivamente al usuario final una solución fácil de usar para que este preste, modifique o retire el consentimiento de manera expresa, clara y sencilla. En particular, el consentimiento debe prestarse mediante una clara acción afirmativa o declaración que establezca una manifestación de acuerdo libre, específica, informada e inequívoca por parte del usuario final, tal como se define en el Reglamento (UE) 2016/679».

91 En ese sentido, Posdzun propone una solución de calificación sofisticada con «guías de datos» de confianza, que podría llevarse a cabo mediante una solución específica en el artículo 5 o a través de las normas antielusión del artículo 11 DMA. Por otro lado, autores como Kerber (2021) defienden la necesidad de ofrecer a los consumidores una opción de uso de las plataformas digitales pagando por ello un precio monetario asequible (o incluso subvencionado), de manera que no tuvieran que usar sus datos personales como moneda de cambio, lo que generaría un mayor control sobre los mismos.

92 En palabras del JURI (Comité de Asuntos Legales) (2021): «Como demuestra el RGPD, los simples regímenes de consentimiento son a menudo insuficientes para hacer frente a la pérdida de control sobre los datos personales por parte de los usuarios. Para limitar las posibles consecuencias negativas para ellos, es necesario impedir que se combinen datos personales».

93 Razón de ello es que un menor *bundling* y *tying* (ya sea por restricciones técnicas o contractuales) limita el aprovechamiento del poder de mercado de una empresa en otros mercados relacionados, lo que permite un mayor intercambio y *multihoming* y abre más oportunidades de negocio a los proveedores de servicios independientes (Kerber, 2021).

el hecho de que tenga esa posición de control exclusivo sobre los datos no implica que deba ser reconocido automáticamente como su propietario legítimo. Esto es lo que aquí se considera injusto y que se pretende corregir devolviendo los beneficios de estos datos a quienes los han generado (Kerber, 2021).

De este modo, y en primer lugar, el artículo 6(2) establece que los *gatekeepers* no utilizarán, en competencia con los usuarios profesionales, ningún dato que no sea públicamente accesible generado en el contexto de su uso de los servicios de plataforma, dado que ello provocaría una ventaja competitiva injusta (considerando 46.º DMA). En segundo lugar, el artículo 6(10) permite a los usuarios empresariales, «de forma gratuita, el acceso efectivo, de calidad, continuo y en tiempo real a los datos agregados o desagregados». Por último, el artículo 6(9) obliga a que los guardianes proporcionen gratuitamente a los usuarios finales la portabilidad efectiva de los datos provistos en el contexto del uso del servicio. Este último derecho va más allá del previsto en el artículo 20 del RGPD (Kerber, 2021), ya que no se limita a los datos personales, sino que abarca los datos en diferentes niveles de agregación y, además, obliga a los guardianes a proporcionar herramientas que faciliten una portabilidad efectiva (a través de API, por ejemplo)[94].

Por último, existen diversas obligaciones particularmente importantes desde la perspectiva del derecho de protección de datos y del consumidor. En primer lugar, la interoperabilidad del artículo 6(7) es relevante de cara a luchar contra el poder económico de las grandes plataformas (Kerber, 2021), ya que no solo permite una mayor competencia, al posibilitar el acceso –por ejemplo, dentro de los ecosistemas– a proveedores de servicios independientes, sino que aumenta las posibilidades de elección de los consumidores[95]. En segundo lugar, en pro de alcanzar una mayor competencia e innovación (Cabral *et al.*, 2021), el artículo 6(11) establece la obligación para el guardián de «proporcionar a terceras empresas proveedoras de motores de búsqueda en línea el acceso en condiciones equitativas, razonables y no discriminatorias[96] a datos sobre clasificaciones, consultas […] generados por los usuarios finales». No obstante, y pese a que la norma dispone que los datos deberán ser anonimizados, existen importantes preocupaciones sobre cómo se llevará a cabo en la práctica para proteger de manera efectiva la privacidad de los usuarios (Kerber y Zolna, 2022). En tercer lugar, y en relación con la dimensión b) (la protección contra la manipulación informativa y del comportamiento) a la que hemos hecho referencia con anterioridad, es necesario que los *gatekeepers* queden sujetos a obligaciones adicionales que protejan la autodeterminación informativa y la autonomía de los usuarios (Kerber, 2021). Sin embargo, este fallo de mercado no se afronta sistemáticamente, ya que las disposiciones del artículo 13 DMA sobre antielusión de las obligaciones de los artículos 5

94 Para una discusión en profundidad, Streel (2021).

95 Sin embargo, esta disposición ha sido criticada por autores como Cabral *et al.* (2021) o Streel (2021) por no ir lo suficientemente lejos en el nivel de protección.

96 Lo que se conoce como términos FRAND.

y 6 no se refieren de forma clara a las estrategias de manipulación informativa (como, por ejemplo, el comportamiento de patrones oscuros). Por lo tanto, no es sorprendente que se hayan presentado propuestas de enmienda (JURI, 2021) para que el uso de patrones oscuros y arquitecturas de elección sesgadas se prohíban directa y explícitamente como parte de las normas antielusión del artículo 13 DMA. Estas prohibiciones podrían entenderse, al mismo tiempo, como un refuerzo directo a la protección del consumidor y de sus datos en el marco de la DMA (Digital Regulation Project, 2021), lo que sería un paso innovador y un gran avance a la hora de integrar las cuestiones de privacidad en el marco del derecho de la competencia.

En cualquier caso, resulta necesario que la DMA tenga en cuenta los objetivos de la privacidad y la protección de datos[97]. Un reconocimiento más explícito en esta norma ayudaría a resolver las contradicciones actuales, a elaborar un enfoque regulador más integrado y, en definitiva, a remediar ambos fallos de mercado y poder hacer frente a los problemas derivados del inmenso poder económico de las grandes plataformas (Kerber y Zolna, 2022).

5.1.3. Derecho de protección de datos

Como hemos comentado, uno de los problemas más importantes reside en la dificultad de los usuarios para otorgar un consentimiento voluntario e informado –debido a la existencia de sesgos de la información y del comportamiento o a la falta de opciones reales para ellos–, lo que, a su vez, vigoriza la recopilación de datos por las grandes plataformas y acaba fortaleciendo su poder de mercado. Si la legislación de protección de datos ayudara a resolver mejor estos problemas, se derivarían importantes consecuencias positivas para la competencia.

Una mayor transparencia, a través de la estandarización de las políticas de privacidad, podría ayudar a que fueran comparables y a que los consumidores identificaran aquellas que se ajustan mejor a sus preferencias (Efroni). Por otro lado, podrían conseguirse numerosos efectos positivos a través de instrumentos como el derecho a la portabilidad de datos del artículo 20 del RGPD –que reduce los costes de intercambio entre plataformas digitales, favoreciendo la competencia (Kerber, 2021)–. Sin embargo, no está claro si será posible resolver estos problemas con los instrumentos existentes o si serán necesarios nuevos tipos de intermediarios (como los PIM) o nuevos sistemas de gestión del consentimiento (Kettner).

[97] *A sensu contrario*, Witt (2021) señala que el artículo 5 a), leído conjuntamente con los considerandos de la DMA, no nos permite concluir que la Comisión considere ahora formalmente la privacidad como un parámetro del bienestar del consumidor u otro tipo de perjuicio relevante en virtud de las normas de competencia.

Otro aspecto para considerar es que, en general, el RGPD sigue un enfoque *único* (o de *one-size-fits-all*[98]). No obstante, algunas de sus disposiciones[99] mantienen un enfoque basado en el riesgo[100], lo que en opinión de autores como Kerber (2021) debería ser un principio básico del reglamento, en el sentido de que debería establecer normas mínimas para cada responsable del tratamiento e incrementar la rigidez de las obligaciones en función del riesgo. Del mismo modo, el TEDH señaló que «cuanto mayor sea la cantidad y la sensibilidad de los datos, más importantes son las garantías que deben aplicarse en las distintas fases del posterior tratamiento» (Kerber, 2021). En este contexto, podría entenderse que existe un mayor riesgo si el consentimiento se ha prestado a una gran plataforma digital, lo que podría contrarrestarse con la imposición de obligaciones más estrictas.

El segundo gran problema a resolver es la aplicación insuficiente de la legislación de protección de datos (Kerber y Zolna, 2022)[101]. Si bien un análisis en profundidad excedería los límites del presente estudio, estamos de acuerdo con el comisario federal de Protección de Datos alemán en la necesidad de establecer una Autoridad Europea de Protección de Datos[102], dotándola de los recursos financieros adecuados y de competencias para evaluar el tratamiento de datos por parte de las grandes plataformas.

5.2. Estrategias de cooperación

Aunque las estrategias unilaterales podrían resolver algunos de los problemas, su eficacia siempre será limitada. Como argumentó el EDPS en 2014 (EDPS, 2014), la elaboración de una estrategia común brindaría soluciones eficaces de cara a hacer frente a los fallos de mercado existentes, especialmente en relación con los mercados de las grandes plataformas (OECD, 2020), cuyo poder económico ya no puede afrontarse desde una sola de las legislaciones, sino que se necesitan recíprocamente para alcanzar sus objetivos (Kerber, 2021). Estas estrategias de cooperación podrían llevarse a cabo no solo mediante la armonización bilateral de las legislaciones de competencia y protección de datos, sino desde un enfoque multilateral,

98 Es decir, todas las empresas reciben el mismo trato, sin perjuicio de sus características particulares.

99 Artículos 30, 34 o 35 del RGPD, por ejemplo.

100 Pese a que este término no está definido en el RGPD, el considerando 75.º indica que se entiende por tal el tratamiento de datos personales que pueda ocasionar daños físicos, materiales o inmateriales a los interesados.

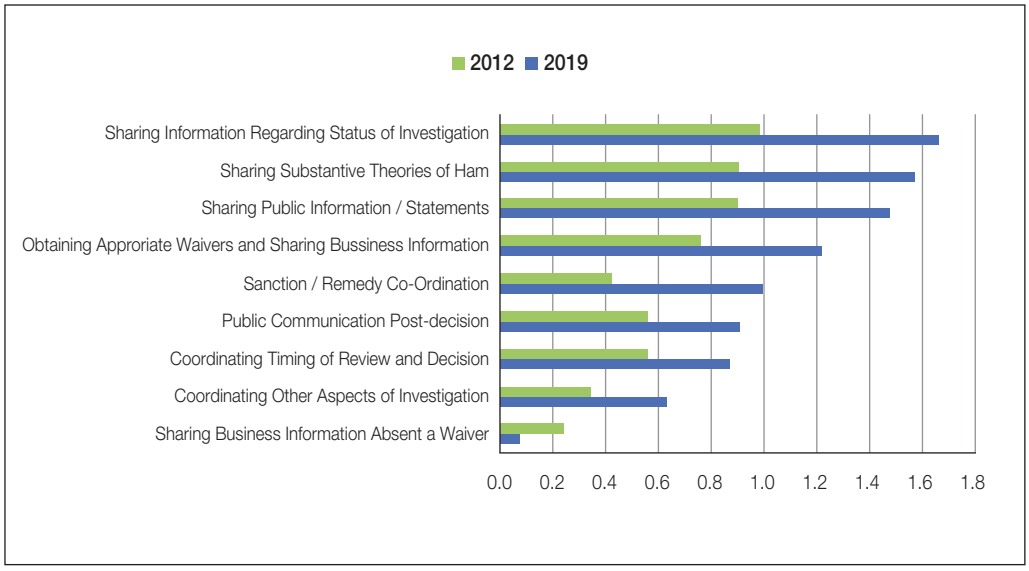
101 El problema de la infraaplicación radica, por un lado, en la inseguridad jurídica inherente a esta ley y, por otro, en la falta de esfuerzos de aplicación por parte de las autoridades de protección de datos individuales (Kerber y Zolna, 2022). Esto, a su vez, puede deberse a la falta de recursos, pero sin duda también a otras razones, como los efectos que provoca el «principio de ventanilla única» y la compleja estructura de competencias resultante. Aunque este principio puede aumentar la seguridad jurídica, también conduce a una aplicación incoherente de la ley en los distintos EM.

102 Stupp.

que incluiría políticas de estandarización (e interoperabilidad), políticas de datos[103] (más allá de las leyes de protección de datos), u otras nuevas normativas que combatan las prácticas comerciales desleales en mercados digitales (UNCTAD, 2021). La DMA podría entenderse como parte de esta estrategia innovadora[104]. Su inconveniente es que se centra en exceso en la legislación de competencia frente a la de protección de datos, perdiendo la oportunidad de aportar un enfoque normativo más integrado (Kerber y Zolna, 2022).

En todo caso, resulta necesario que los expertos de ambas disciplinas colaboren de manera conjunta, lo que parece haberse producido de manera paulatina en los últimos años. El gráfico de más abajo ilustra que, en todas las categorías de cooperación, la frecuencia ha aumentado entre 2012 y 2019, destacando especialmente el intercambio de información entre autoridades sobre el estado de la investigación, las teorías sustantivas del perjuicio o la información pública.

Gráfico 1. **Cooperación entre autoridades de competencia**[105]



[103] Iniciativas como la DSA o la propuesta de la Ley de datos, cuyos principales objetivos residen en garantizar la equidad en el entorno digital y permitir a los consumidores y empresas tener un mayor control sobre sus datos, estimular un mercado de datos competitivo e impulsar la innovación (Eversheds Sutherland, 2021).

[104] Con el fin de hacer frente a las cuestiones de regulación cruzada, se han creado organismos como el European Digital Clearinghouse o el Grupo de Alto Nivel (art. 40 DMA), que ayudará a la Comisión en la aplicación de esta norma.

[105] OECD/ICN (2021).

Sin embargo, la mayor parte se ha producido entre autoridades a nivel nacional[106]. El Gobierno británico ha creado diversos organismos para promover que las autoridades sobre protección de datos –la Oficina del Comisario de Información (ICO, por sus siglas en inglés)– y sobre competencia –la CMA– adopten un enfoque coordinado y estratégico (Eversheds Sutherland, 2021). Ya en 2020, el Foro de Cooperación para la Regulación Digital (o DRCF), un proyecto conjunto entre la ICO, la CMA, la Autoridad de Conducta Financiera (o FCA) y la Oficina de Comunicaciones (u Ofcom), se puso en marcha para promover la cooperación y «permitir una regulación de la economía digital coherente, informada y receptiva». Su Plan de Trabajo (Digital Regulation Cooperation Forum, 2021) para 2021 y 2022 detalla sus prioridades, entre las que se encuentran la regulación del procesamiento algorítmico[107] y la introducción de un código de conducta exigible a empresas con estatus de mercado estratégico (SMS), con la correspondiente creación de un nuevo organismo regulador (la Unidad de Mercados Digitales[108] o DMU). Por su parte, el informe Penrose (2021) recomendó la creación de una Unidad de Monopolios de Red y Datos que sustituya a la mencionada DMU y cuyas competencias estén separadas de las de la CMA. El informe señaló que «el mandato de esta Unidad de ocuparse de los efectos de los monopolios de datos sobre la competencia y los consumidores se cruzará inevitablemente con la Oficina del Comisionado de Información (ICO) siempre que se trate de cuestiones de privacidad». De este modo, esta nueva unidad dará pie a una mayor colaboración entre la CMA y la ICO. En relación con el reciente proyecto de Ley sobre seguridad en línea (*Online Safety Bill*)[109], dichos organismos emitieron una declaración conjunta (CMA y Ofcom, 2022) en la que hicieron referencia a tres posibles interacciones (sinergias y tensiones políticas, y restricciones innecesarias) que podrían producirse entre el ámbito de la competencia y el de la seguridad *online* (Eversheds Sutherland, 2022).

Sin embargo, a nivel europeo, la cooperación entre las autoridades de competencia y protección de datos solo se ha producido en seis casos[110] (Carugati, 2022). La primera se

[106] Francia puso en marcha en 2020 el Pôle d'Expertise de la Régulation Numérique (PEReN), que se encarga de asistir a las administraciones estatales (incluida la autoridad francesa de competencia) para abordar los problemas digitales.

[107] Partiendo del informe de la CMA: *Algorithms: How they Can Reduce Competition and Harm Consumers*, UK Government (2021).

[108] Organismo integrado en la CMA, se encargaría de imponer medidas de intervención que favorezcan la competencia y la innovación, incluyendo medidas relacionadas con los datos y su portabilidad.

[109] Online Safety Bill, originated in the House of Commons the 15th December 2020, to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes. Bill 220 58/3. UK Parliament.

[110] Todos ellos son procedimientos en virtud de la legislación antimonopolio, como las investigaciones de Google Privacy Sandbox de la UE y el Reino Unido, la investigación francesa sobre el TCA de Apple, el caso francés de GDF Suez y el caso alemán de Meta. Solamente existe un caso relativo a una fusión: la revisión de la fusión Google/Fitbit de la CE.

produjo en 2014 en el caso GDF Suez (ahora Engie), en el que para implementar la decisión propuesta por la autoridad de competencia de que esta empresa compartiera algunos datos de sus clientes con los competidores, la autoridad de protección de datos emitió un dictamen para definir cómo podía llevarlo a cabo sin menoscabar la privacidad (Carugati, 2022). El segundo ejemplo de cooperación se produjo en 2016 en el caso alemán Meta[111], donde el abogado general Rantos alegó que «una autoridad de competencia, en el marco de sus facultades en virtud de las normas de competencia, puede examinar, como cuestión incidental, la conformidad de las prácticas investigadas con las normas del RGPD, teniendo en cuenta cualquier decisión de la autoridad de control competente sobre la base del RGPD, informando y, en su caso, consultando a dicha autoridad»[112]. El TJUE, en su reciente Sentencia de 4 de julio de 2023[113], confirmó finalmente dicha postura, lo que ha supuesto un importante cambio en la jurisprudencia sentada en el caso Asnef-Equifax[114]. Por último, el caso Google Privacy Sandbox en el Reino Unido nos ha ofrecido la forma más avanzada de cooperación hasta la fecha (Carugati, 2022). En este, las autoridades han trabajado estrechamente para garantizar la coherencia entre sus decisiones y supervisar que el desarrollo de las propuestas del *sandbox* de privacidad de Google proteja tanto a la competencia como a la privacidad (Carugati, 2022).

En resumen, creemos que únicamente una fuerte colaboración entre ambas legislaciones podría solventar los fallos de mercado y lograr alcanzar con éxito sus respectivos objetivos, por lo que su establecimiento debería ser prioritario en la agenda de las autoridades y organismos internacionales[115].

6. Conclusión

El advenimiento de la economía digital ha favorecido notablemente la innovación pero, como hemos observado, también ha desencadenado un importante examen de conciencia entre los expertos[116]. Los datos personales se han convertido en uno de los más valiosos

---

111 B6-22/16 Facebook, February 6, 2019, para. 555.

112 C-252/21 (NormaCEF NCJ066690) *Meta Platforms and Others, Opinion of Advocate General Rantos*, September 20, 2022, para. 33.

113 STJUE, de 4 de julio de 2023, asunto C-252/21 (Meta Platforms Inc.) (NormaCEF NCJ066690).

114 C-238/05 *Asnef-Equifax vs. Asociación de Usuarios de Servicios Bancarios (Ausbanc),* ECLI:EU:C:2006:734, November 23, 2006, para. 63 (NormaCEF NCJ040569).

115 Organismos como la Red de Cooperación Internacional están trabajando en ello, por ejemplo, en su proyecto: International Competition Network, Scoping paper (2021). *Competition Law Enforcement at the Intersection Between Competition, Consumer Protection, and Privacy*, Paper for ICN Steering Group.

116 En ese sentido, Schweitzer *et al.* (2018), Crémer *et al.* (2019), Furman *et al.* (2019), ACCC (2019) y Stigler Committee on Digital Platforms (2019).

activos y en una fuente de poder de mercado[117], garantizando a las plataformas poseedoras el disfrute de ventajas competitivas únicas. Como consecuencia, y mediante el potencial abuso de su *data power*[118], podrían encontrarse en una situación privilegiada no solo para recurrir a prácticas desleales y de explotación frente a los usuarios (fallo de mercado), sino también para perfilar e influenciar –ilícitamente– la libre formación de sus opiniones (fallo informacional y del comportamiento) (Kerber, 2021). Ambos problemas se encuentran profundamente entrelazados porque, por un lado, son las características económicas de estas plataformas las que les permiten recabar una gran cantidad de datos personales y, por otro, este acceso privilegiado (Kerber, 2021) conduce a un mayor afianzamiento de su poder económico a través de (a) el aumento de las barreras de entrada y la exclusión de competidores, y (b) el aprovechamiento de la asimetría de información entre dichas empresas y los usuarios para llevar a cabo estrategias de manipulación informativa y conductual (OECD, 2020). Todo ello nos lleva a afirmar que existe un vínculo familiar (Costa-Cabral *et al.*, 2017) entre el derecho de competencia[119] y el de protección de datos, vínculo que justificaría que las autoridades de competencia tuvieran en cuenta –de manera complementaria– el impacto sobre la privacidad[120] y la protección de datos, al evaluar las conductas empresariales en virtud de las normas de competencia[121].

No obstante, el debate se encuentra abierto y no existe una postura clara. En el pasado la CE siempre había considerado que el deterioro de la privacidad no era una forma relevante de perjuicio con arreglo a la legislación de competencia, como ejemplifica el asunto Facebook/WhatsApp de 2014. Más recientemente, la posición de las autoridades ha ido evolucionando hasta llegar a la Sentencia de 3 de julio de 2023 en el asunto Meta Platforms, en que el TJUE defendió que una autoridad de competencia tiene la capacidad para examinar y constatar, en el marco de un procedimiento sancionador por abuso de posición dominante, si las condiciones generales del servicio de la empresa investigada relativas al tratamiento de datos personales, y la aplicación de esas condiciones, son conformes al RGPD, siempre y cuando dicho pronunciamiento sea necesario para declarar

117 Con su reconocimiento explícito en el artículo 18(3a) GWB.

118 El Comité Europeo de Protección de Datos hizo referencia a la acumulación de *poder informacional* por parte de las compañías como parámetro a tener en cuenta a la hora de evaluar los impactos de una concentración económica.

119 Para un resumen de los problemas sobre competencia y sus potenciales efectos perjudiciales: capítulo 1 del informe Furman (Furman *et al.*, 2019).

120 En palabras de Robertson: «Los consumidores no suelen tener voz real en cuestiones de privacidad como parte de la calidad de un producto online, ya que normalmente no pueden eludir a los proveedores de servicios digitales predominantes».

121 Ya en 2014, el Supervisor Europeo de Protección de Datos argumentó acerca de la importancia de la privacidad y la protección de datos como factores centrales en la evaluación de las actividades empresariales y en su correspondiente impacto en la competitividad, la eficiencia del mercado y el bienestar de los consumidores (EDPS, 2014).

la existencia del abuso investigado[122]. Sin perjuicio de la enorme importancia que posee dicha decisión, que amplía las facultades de apreciación de las autoridades de competencia y reconoce explícitamente su capacidad para declarar infracciones del RGPD en el marco del examen de un abuso de posición dominante, es muy probable que el debate sobre el objetivo correcto de la legislación de competencia continúe mucho más allá de los casos que hemos analizado.

Con todo, creemos que únicamente una sólida colaboración (Stucke y Grunes, 2016) entre autoridades podría ayudar a solventar los fallos de mercado y a alcanzar sus respectivos objetivos, por lo que su establecimiento debería ser prioritario en la agenda de autoridades y organismos internacionales[123]. Todo ello podría ayudar a identificar las posibles conductas ilícitas con mayor antelación (incluso antes de que se cometieran), a compartir el conocimiento adquirido y a disminuir las posibles ineficiencias. No obstante, estas recomendaciones presentan desafíos en términos de su aplicación práctica –posibles discrepancias o conflictos entre autoridades de las distintas ramas legales (Furman *et al.*, 2019)–. Una respuesta íntegra a estos retos requiere futuras investigaciones y una revisión de la legislación de competencia (y sus interrelaciones con otras ramas del derecho) que se adapte a los mercados digitales del siglo XXI (EDPS, 2014) –donde iniciativas como la DMA a nivel europeo o la reciente redacción de la Sec. 19a GWB en el marco de la legislación alemana suponen importantes avances–.

[122] STJUE de 4 de julio de 2023, asunto C-252/21 (Meta Platforms Inc.).

[123] Organismos como la Red de Cooperación Internacional están trabajando en ello, por ejemplo, en su proyecto International Competition Network, Scoping paper (2021). *Competition Law Enforcement at the Intersection Between Competition, Consumer Protection, and Privacy*, Paper for ICN Steering Group.

Referencias bibliográficas

ACCC (Australian Competition and Consumer Commission). (2019). *Digital Platforms Inquiry. Final Report*.

Brokelmann, H. (2006). La negativa de suministro y figuras afines. En *Abuso de Posición de Dominio* (pp. 341-365).

Bundeskartellamt. (2019). Bundeskartellamt prohibits Facebook from combining user data from different sources. www.Bundeskartellamt.de

Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T. M. y Alstyne, M. W. van (2021). *The EU digital markets act: a report from a panel of economic experts*. Publications Office of the European Union.

Calvano, E. y Polo, M. (2021). Market power, competition and innovation in digital markets: A survey. *Information Economics and Policy*, *54*, 100853.

Carugati, C. (2022). Overview of Privacy in Cases Relevant to Competition. *SSRN 4243506*.

CMA y Ofcom (2022). Online Safety and Competition in Digital Markets: A Joint Statement between the CMA and Ofcom.

Condorelli, D. y Padilla, J. (2020). Harnessing platform envelopment in the digital world. *Journal of Competition Law & Economics*, *16*(2), 143-187.

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), 11-50.

Crémer, J., Montjoye, Y. A. de y Schweitzer, H. (2019). Competition policy.

Digital Regulation Cooperation Forum (2021). Plan of Work for 2021 to 2022.

Digital Regulation Project (2021). Consumer Protection for Online Markets and Large Digital Platforms. *Policy Discussion Paper*, *1*.

EDPS. (2014). Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy. Preliminary Opinion of the European Data Protection Supervisor.

Ezrachi, A. y Robertson, V. H. (2019). Competition, market power and third-party tracking. *World Competition*, *42*(1).

Forrest, K. B. (2019). Big Data and online advertising: emerging competition concerns. *CPI Antitrust Chronicle*.

FTC (Federal Trade Commission). (2012). FTC Approves Final Settlement with Facebook: Facebook Must Obtain Consumers' Consent Before Sharing their Information Beyond Established Privacy Settings.

Furman, J., Coyle, D., Fletcher, A., McAuley, D. y Marsden, P. (2019). *Unlocking digital competition: Report of the digital competition expert panel*. UK government publication, HM Treasury, 27.

Gilbert, P. y Pepper, R. (2015). Privacy considerations in European Merger Control: A square peg for a round hole. *Competition Policy International*.

Graef, I., Clifford, D. y Valcke, P. (2018). Fairness and enforcement: Bridging competition, data protection, and competition law. *International Data Privacy Law*, *8*(3), 200-223.

Jones Harbour, P. (2007). Dissenting Statement of Commissioner Pamela Jones Harbour: In the Matter of Google/DoubleClick.

JURI (Committee on Legal Affairs). (2021). Draft opinion on the proposal for a regulation of the European Parliament and of the Council Contestable and fair mar-

kets in the digital sector (Digital Markets Act). (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)).

Kerber, W. (2021). Competition law in context: the example of its interplay with data protection law from an economic perspective. *Wirtschaft und Wettbewerb*, *7*(8).

Kerber, W. y Specht-Riemenschneider, L. (2021). Synergies between data protection law and competition law. *SSRN 3977039*.

Kerber, W. y Zolna, K. K. (2022). The German Facebook case: The law and economics of the relationship between competition and data protection law. *European Journal of Law and Economics*, *54*(2), 217-250.

Körber, T. (2016). Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law. *NZKart*, *303*.

Körber, T. (2018). Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law. *NZKart 2016*.

Lynskey, O. (2018). Non-price Effects of Mergers.

Maggiolino, M. y Ferrari, G. (2020). Can Digital Data be Replaced? Data, Competition Policy International.

OECD (2018). Quality Considerations in the Zero-Price Economy.

OECD (2020). Consumer Data Rights and Competition. Background note.

OECD (2022). The Evolving Concept of Market Power in the Digital Economy. OECD Competition Policy Roundtable Background Note.

OECD/ICN (2021). OECD/ICN Report on International Co-operation in Competition Enforcement.

Pecman, J., Johnson, P. y Reisler, J. (2020). Essential facilities fallacy: Big tech, winner-take-all markets, and anticompetitive effects. *Competition Policy International*, 1-12.

Penrose, J. (2021). *Power to the People: Independent Report on Competition Policy*. Department for Business, Energy & Industrial Strategy, UK Government.

Robertson, V. H. (2020). Excessive data collection: privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1).

Robles Martín-Laborda, A. (2021). Inteligencia artificial y personalización de precios. En *Perspectiva legal y económica del fenómeno FinTech* (pp. 573-598). Wolters Kluwer.

Rubinfeld, D. L. y Gal, M. S. (2017). Access barriers to big data. *Ariz. L. Rev.*, *59*, 339.

Schweitzer, H. (2021). The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Markets Act Proposal. *Forthcoming, ZEuP*, *3*.

Schweitzer, H., Haucap, J., Kerber, W. y Welker, R. (2018). *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*. Nomos Verlagsgesellschaft mbH & Co.

Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*, 1.880-1.903.

Stigler Committee on Digital Platforms. (2019). *Final report*, *16*.

Streel, A. de, Feasey, R., Kraemer, J. y Monti, G. (2021). Making the Digital Markets Act more resilient and effective. *SSRN 3853991*.

Stucke, M. E. (2018). Should we be concerned about data-opolies? *Geo. L. Tech. Rev.*, *2*, 275.

Stucke, M. E. (2022). Breaking away: How to regain control over our data, privacy, and autonomy. *Oxford University Press*.

Stucke, M. E. y Grunes, A. P. (2016). Big Data and Competition Policy (pp. 325-334). *Oxford University Press*.

Swire, P. (2007). Protecting Consumers: Privacy matters in antitrust analysis. *Center for American Progress*, *19*(10), 07.

Tucker, C. (2018). Network effects and market power: what have we learned in the last decade? *Antitrust*, *32*(2), 72-79.

UNCTAD. (2021). Las leyes, políticas y normativas de protección del consumidor en respuesta a la pandemia de COVID-19 y después de esta. *Nota de la secretaría de la UNCTAD.*

Witt, A. (2021). Data, Privacy and Competition Law. *Graz Law Working Paper*, *24*.

Nina Polit Sobrino. Titulada en Economía y Derecho por la Universidad Carlos III de Madrid, actualmente desempeña un puesto de graduada en el Departamento de Derecho Financiero de Uría Menéndez. Recibió el primer premio al TFG por parte de la Cátedra de Investigación Cuatrecasas-UC3M. Realizó dos estancias, en la Universidad Bocconi y en la Universidad de California, San Diego, donde trabajó como asistente de investigación en el Departamento de Economía bajo la dirección del profesor emérito James E. Rauch. https://orcid.org/0009-0000-2601-0336