La competencia y la protección de datos personales en el ámbito digital

Febrero de 2026

AC CO Autoritat Catalana de la Competència

Generalitat de Catalunya

1. Introducción

Con la creciente importancia de los mercados digitales, también ha crecido la preocupación por la privacidad y la protección de los datos personales. Además, bajo determinadas circunstancias, algunas infracciones en esta materia pueden estar relacionadas con infracciones de la normativa de competencia.

En este contexto, la Autoridad Catalana de la Competencia (en adelante, ACCO) incluyó en el Programa de actuaciones de promoción de la competencia 2025 - 2026 la elaboración de un estudio sobre la competencia y la protección de los datos personales, con el objetivo de aportar información sobre las interacciones de las normativas de protección de datos de carácter personal y de competencia, en los mercados digitales, que pueda resultar de utilidad para las empresas, los usuarios o las autoridades de competencia.

Por este motivo, la ACCO encargó a la Dra. Alba Ribera Martínez, profesora de Derecho de la Competencia y Análisis Económico del Derecho en la Universidad Villanueva (Madrid), la realización de un estudio sobre estas materias. Este documento recoge las partes más relevantes para la ACCO, desde el punto de vista de la política de competencia, del ***"Estudio sobre la competencia y la protección de datos personales en el ámbito digital"***, elaborado por la Dra. Ribera[1].

[1] Véase el estudio completo (Ribera, 2025) en el siguiente enlace: https://acco.gencat.cat/permalink/e6abffc3-073c-11f1-9a91-005056ba51b2.pdf. Cualesquiera errores, omisiones o inexactitudes como consecuencia de la síntesis del estudio son responsabilidad exclusiva de la ACCO.

2. Contexto

La creciente digitalización de la economía ha provocado que el acceso a datos por parte de las empresas, entre ellos los datos personales[2], sea fundamental en la mayoría de los modelos de negocio en los mercados digitales. Los datos constituyen un recurso estratégico y son utilizados para obtener ventajas competitivas. Estas ventajas dependen de la capacidad de almacenamiento, procesamiento y utilización de los datos por parte de los operadores, así como de la calidad de los datos. En este sentido, existe una gran diferencia entre los operadores digitales de menor tamaño y las grandes plataformas digitales que acceden a un gran volumen de datos y aprovechan las economías de escala y alcance a su favor.

Pese a su naturaleza no excluyente, algunas empresas pueden optar por reservar la propiedad de los datos que generan y no compartirlos ni venderlos a otros operadores, lo que puede implicar grandes ventajas competitivas. Por otro lado, existe una barrera de acceso a estos datos debido a que la normativa de protección de datos personales impone limitaciones a todos los operadores económicos. El Reglamento General de Protección de Datos (en adelante, RGPD)[3] es la norma europea que regula el tratamiento de datos personales y reconoce el derecho a su protección a los ciudadanos[4]. Solamente resulta aplicable al tratamiento de los datos personales[5] y, de esta manera, predetermina la mayor o menor dificultad con la que los operadores económicos pueden acceder a distintos tipos de datos.

[2] El artículo 4 del Reglamento General de Protección de Datos (RGPD) define los "datos personales" como toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

[3] 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. Tiene alcance general y eficacia directa, por lo que se aplica en todos los Estados miembros. Sin embargo, Ribera (2025) señala que, con el fin de asegurar la seguridad jurídica sobre la materia en el territorio nacional, el legislador introdujo la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que no añade nada nuevo al RGPD en cuanto a su diseño regulatorio, ya que solamente clarifica algunos aspectos que el Reglamento dejaba abiertos, si bien incluye en su Título X una serie de derechos digitales que exceden de aquellos que ya estaban originariamente previstos en el RGPD.

[4] Ribera (2025) destaca la naturaleza del derecho a la protección de datos personales como un derecho fundamental, reconocido en la Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8, de forma separada al derecho al respeto de la vida privada y familiar de los ciudadanos. El derecho a la protección de los datos personales se conforma en torno a una estructura tripartita que exige: (i) el respeto a una serie de principios para el procesamiento de datos; (ii) la asignación de unos derechos al interesado sobre el que se realiza el tratamiento; y (iii) la obligación de que su supervisión se garantice a través de una autoridad independiente. Otorga un control sobre el tratamiento al interesado, pero eso no quiere decir que el interesado (o el responsable del tratamiento) sea el propietario de estos datos.

[5] El artículo 4 del RGPD define el "tratamiento" como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Ante esta situación, las herramientas clásicas del Derecho de la competencia son insuficientes para capturar los efectos de la acumulación masiva de datos, los fenómenos de retroalimentación propios de los ecosistemas digitales o la explotación de los usuarios a través de condiciones contractuales desequilibradas.

La heterogeneidad de los datos y sus diferencias según el sector del cual se trate impiden un enfoque uniforme, requiriendo un análisis caso por caso sobre su relevancia competitiva. Es decir, la importancia de los datos personales y su relevancia como parámetro de competencia dependerán de las particularidades de cada uno de los mercados digitales y de los tipos de datos necesarios para ser tratados en cada caso.

En este contexto, la Comisión Europea introdujo el Reglamento de Mercados Digitales[6] y el Reglamento de Servicios Digitales[7], dos normas de regulación ***ex ante*** que complementan la normativa de competencia. Posteriormente, también se aprobó el Reglamento de Inteligencia Artificial[8].

En el caso de Cataluña, la digitalización empresarial avanza a gran velocidad: cerca de un tercio de las ventas de las compañías con más de 10 trabajadores ya se realizan a través de comercio electrónico, mientras que un 46,8% depende de servicios de computación en la nube. Además, más de 400.000 operadores del tejido empresarial catalán emplean tecnologías de inteligencia artificial para márketing, gestión o procesos productivos[9]. Esta fuerte adopción tecnológica convierte a Cataluña en un polo de atracción de talento digital y en un espacio particularmente sensible a los efectos competitivos asociados al control y tratamiento de datos.

Cataluña también cuenta con aproximadamente 25.000 empresas tecnológicas que representan el 14% del PIB autonómico[10], y más del 9% constituidas como ***start-ups*** de reciente creación[11], consolidándose

[6] 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.
[7] 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.
[8] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828. Otras normas relevantes en el ámbito digital son el Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos); y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Para más información, véase Ribera (2025).
[9] Véanse: Enquesta sobre l'ús de TIC i del comerç electrònic a las empreses 2023-2024. Empreses de 10 ocupats o més. Per sector d'activitat i realització de vendes. https://www.idescat.cat/pub/?id=eticce2324&n=2.11.2.1.2; Enquesta sobre l'ús de TIC i del comerç electrònic a las empreses 2023-2024. Empreses de 10 ocupats o més. Per sector d'activitat i serveis d'informàtica al núvol. https://www.idescat.cat/pub/?id=eticce2324&n=2.07.2; Enquesta sobre l'ús de TIC i del comerç electrònic a les empreses 2023-2024. Empreses de menys de 10 ocupats. Per tecnologies d'intel·ligència artificial. https://www.idescat.cat/pub/?id=eticce2324&n=1.09.1; y Enquesta sobre l'ús de TIC i del comerç electrònic a les empreses 2023-2024. Empreses de 10 ocupats o més. Per sector d'activitat i tecnologies d'intel·ligència artificial. https://www.idescat.cat/pub/?id=eticce2324&n=2.09.1.2; del Instituto de Estadística de Cataluña.
[10] Govern de Catalunya. (4 de marzo de 2024) Creix un 14% el volum de negoci de les empreses catalanes del sector tecnològic i digital que arriba fins als 40.000 milions d'euros. Govern.cat, https://govern.cat/salapremsa/notes-premsa/686362/creix-14-percent-volum-negoci-empreses-catalanes-del-sector-tecnologic-digital-que-arriba-fins-als-40000-milions-deuros.
[11] ACCIÓ. (2025). El sector tecnològic i digital a Catalunya. https://www.accio.gencat.cat/web/.content/bancconeixement/documents/pindoles/ACCIO-sector-tecnologic-digital-catalunya-2025-ca.pdf.

como referente del sur de Europa. No obstante, pese al dinamismo innovador catalán, los mercados digitales más lucrativos (publicidad online, sistemas operativos y redes sociales) están dominados por grandes plataformas estadounidenses y chinas, relegando la innovación catalana a servicios complementarios o anexos a estos mercados.

Además, la concentración de recursos digitales en grandes plataformas genera riesgos para el ecosistema catalán de ***start-ups deep tech***[12], que a menudo carecen del mismo acceso a datos que los grandes actores internacionales.

[12] Empresas emergentes que desarrollan tecnologías altamente innovadoras, con fuerte base científica o de ingeniería.

3. Interacción entre la defensa de la competencia y la protección de los datos personales

Las potenciales infracciones de la normativa de competencia

En cuanto a las potenciales infracciones de la normativa de competencia con relación al tratamiento de datos personales, las principales conductas son, por un lado, **las estrategias de exclusión mediante la denegación de acceso a datos necesarios para competir en mercados aguas abajo y, por el otro, las condiciones desequilibradas que algunos operadores imponen a sus usuarios en materia de protección de datos personales,** como la imposición de cláusulas de consentimiento opacas o poco equitativas que restringen la libertad de elección de los usuarios[13].

La protección de los datos personales como parámetro de competencia

Cabe destacar que la Comisión Europea ha reconocido que la privacidad es un aspecto de la calidad de un producto o servicio[14] y que se debe considerar dentro del análisis de competencia, ya que los consumidores perciben el grado de protección de sus datos personales como una manifestación de su capacidad de elección en este tipo de mercados[15].

El Tribunal de Justicia de la Unión Europea (en adelante, TJUE) también ha señalado que el acceso a los datos personales y su explotación tienen una gran importancia en el marco de la economía digital y que, por este motivo, se han convertido en un parámetro significativo de la competencia entre empresas de la economía digital[16]. Por lo tanto, **la protección de los datos personales es**

[13]En ambos casos se trataría de un abuso de posición dominante y, por lo tanto, de una infracción del artículo 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, o del artículo 102 del Tratado de Funcionamiento de la Unión Europea.

[14] Véase la Comunicación de la Comisión relativa a la definición de mercado de referencia a efectos de la normativa de la Unión en materia de competencia (C/2024/1645).

[15] Véase el Caso M.8124, Microsoft/LinkedIn. C(2016) 8404 final.

[16] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt.

un parámetro de competencia. Más allá del precio o la innovación, los consumidores valoran el grado de control sobre sus datos personales como un factor de calidad de los servicios digitales.

Las teorías del daño que se han explorado

Se pueden destacar dos categorías de teorías del daño: (i) **la negativa a proporcionar acceso a una infraestructura indispensable, como abuso de exclusión**, y (ii) **la imposición de condiciones de transacción injustas e inequitativas, como abuso de explotación**.

Por lo que respecta a la primera conducta, se debe tener en cuenta que el RGPD limita la atribución de derechos de propiedad sobre los datos personales, trasladando a la autoridad de competencia la tarea de modular el acceso y uso de esos datos. Es decir, el RGPD no confiere un derecho de propiedad ni al interesado ni al responsable del tratamiento sobre esos datos[17]. Por lo tanto, al aplicar esta teoría del daño, la responsabilidad de definir y modular los derechos del responsable del tratamiento se traslada inmediatamente a la autoridad de competencia (y no a la autoridad de protección de datos).

La denegación de acceso a datos personales puede constituir abuso de posición dominante si impide la competencia en mercados aguas abajo, pero requiere demostrar la indispensabilidad del input y la eliminación total de competencia. Ahora bien, el TJUE en el caso *Android Auto*[18] flexibilizó esta jurisprudencia consolidada, ya que la **infraestructura se consideró esencial cuando formaba parte de un ecosistema abierto a terceros**, permitiendo adaptar los requisitos de indispensabilidad según el contexto. El TJUE flexibiliza la aplicación de la jurisprudencia para aquellas empresas que desarrollan sus infraestructuras para conformar un ecosistema en el que participan empresas terceras en mercados descendentes o complementarios del mercado principal en el que opera la empresa dominante.

Este es uno de los elementos que, según la jurisprudencia del TJUE, debe tenerse en cuenta para considerar aquellas situaciones de negativa de acceso a datos personales de ahora en adelante. Ante aquellas situaciones en las que los ecosistemas de las empresas dominantes estén abiertos a la participación de empresas terceras, el TJUE introduce una suerte de derecho para participar en las condiciones más favorables al solicitante de acceso a esa infraestructura.

En cuanto a la segunda conducta, las autoridades nacionales de competencia han aplicado la figura del abuso explotativo a prácticas vinculadas al tratamiento de datos personales, usando el RGPD como indicio relevante para evaluar conductas anticompetitivas[19]. De hecho, en una cuestión prejudicial emitida por el TJUE, en relación con el caso *Facebook* de la autoridad de competencia alemana, se confirmaba que **la conformidad de las actividades de la empresa dominante con las disposiciones del RGPD puede constituir un indicio relevante para determinar si estas constituyen medios que rigen una competencia normal y para evaluar las consecuencias de una determinada práctica en el mercado o para los consumidores[20]**.

[17] El derecho a la protección de datos personales garantiza el control del interesado sobre el tratamiento de sus datos (autodeterminación informacional), pero no supone un derecho de propiedad. Los modelos de negocio digitales basados en datos personales no implican una transmisión de propiedad de los datos, sino un régimen de derechos limitados sujetos a las bases legales y principios del RGPD.

[18] Véase el Caso C-233/23, Alphabet y otros. ECLI:EU:C:2025:110.

[19] Véanse los casos B6-22/16. Abusive business terms due to inappropriate data processing, del Bundeskartellamt; 25-D-02. Practices implemented in the sector for mobile application advertising on iOS devices, de la Autorité de la Concurrence; y S/0005/21, Booking de la Comisión Nacional de los Mercados y la Competencia.

[20] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 47.

Los incumplimientos de la normativa de protección de datos como infracciones de competencia

En términos generales, para determinar la existencia de una conducta anticompetitiva y, en concreto, la infracción de la prohibición de abuso de posición dominante, una autoridad de defensa de la competencia debe apreciar, teniendo en cuenta todas las circunstancias del caso concreto, si las actividades de la empresa en posición dominante producen el efecto de obstaculizar, por medios diferentes de los que rigen una competencia normal de productos o servicios, el mantenimiento del nivel de competencia que aún exista en el mercado o el desarrollo de esa competencia[21].

Por lo tanto, el RGPD es uno de los elementos que deben considerarse insertos en esa cláusula de atender "a todas las circunstancias" del caso concreto, pero, en principio, no es el elemento determinante que establece la existencia de una infracción en materia de competencia. Es decir, **una infracción del RGPD no puede ser, de forma aislada, el único elemento en favor de la determinación de la responsabilidad de la empresa dominante respecto de su conducta anticompetitiva**.

No obstante, las autoridades nacionales de competencia amplían la interpretación de conductas abusivas explotativas, incorporando elementos como la neutralidad de interfaces y los desequilibrios informacionales entre operadores dominantes y usuarios.

El consentimiento prestado por los consumidores para acceder a servicios digitales

La normativa de protección de datos personales obliga a los responsables de tratamientos de datos personales al cumplimiento de los requisitos legales que se establecen en el RGPD. Entre estos se encuentra el consentimiento, concebido como una de las bases legales del tratamiento de datos personales –artículo 6.1.a) del RGPD.

Este consentimiento puede convertirse en una herramienta de dominio cuando no existen alternativas reales para el consumidor. De hecho, **cuando se trata de grandes plataformas digitales, los perjuicios por infracciones de protección de datos, en relación con el consentimiento del interesado para el tratamiento de los datos personales, pueden equipararse a daños anticompetitivos**, especialmente en el contexto del Reglamento de Mercados Digitales.

Los principios generales de la normativa de protección de datos personales

Adicionalmente de las bases legales contempladas en el artículo 6 del RGPD, el artículo 5 del Reglamento establece una serie de principios. Ahora bien, estos principios no pueden sustentar, cuando se consideran de forma aislada, una infracción en materia de competencia. Es decir, **no podemos derivar directamente que la violación de uno de los principios del RGPD sea suficiente para fundamentar la existencia de una infracción en materia de competencia**.

[21] Véase el Caso C-152/19 P, Deutsche Telekom AG contra Comisión Europea. ECLI:EU:C:2021:238, párrafos 41 y 42.

Este es un límite importante que debemos reseñar en la interacción entre ambas disciplinas, ya que no todos los incumplimientos de la normativa en protección de datos son suficientemente relevantes para fundamentar la existencia de una infracción en materia de competencia.

La conformidad de la normativa de protección de datos personales para el examen de abuso de posición dominante

La consideración del RGPD en el análisis de competencia no está excluida, ya que las autoridades de competencia no suplantan las funciones ni competencias de las autoridades de protección de datos[22]. Ninguna disposición del RGPD prohíbe que las autoridades nacionales de competencia concluyan, en el ejercicio de sus funciones, que un tratamiento de datos efectuado por una empresa en posición dominante es susceptible de constituir un abuso cuando no es conforme con el RGPD. Al ejercer funciones distintas y perseguir objetivos también diferentes, la autoridad de protección de datos y la autoridad de competencia pueden confluir en la aplicación de las normas que deben interpretar respecto de un mismo caso. Por una parte, la autoridad de protección de datos se encargará de controlar la aplicación del RGPD con el fin de proteger los derechos y libertades fundamentales recogidos por este. Por otra parte, la autoridad de competencia analizará si debe declarar la existencia de una infracción de competencia.

Dando por sentado que la interacción de ambas disciplinas está normativa y sustantivamente aceptada (o, al menos, no está prohibida), es más complejo establecer el nexo causal entre la manifestación del poder de mercado del operador dominante y la existencia de la infracción en materia de competencia cuando se deriva de un incumplimiento en materia de protección de datos.

La autoridad alemana de competencia considera que para determinar la existencia de un abuso de posición dominante solamente es exigible que se pruebe la causalidad normativa entre la dominancia y la conducta. Es suficiente que la conducta genere efectos anticompetitivos como resultado de la dominancia[23].

La autoridad francesa también ha acogido este requisito de causalidad normativa, bajo la premisa de que la jurisprudencia europea no requiere que exista un nexo causal entre la dominancia y las condiciones impuestas por el operador dominante cuando nos encontramos ante un abuso de tipo explotativo[24]. No obstante, el Tribunal General ha señalado recientemente que los efectos anticompetitivos deben ser, al menos, atribuibles a la conducta abusiva del operador dominante[25].

El incumplimiento de otras normas como una restricción anticompetitiva

El TJUE ha defendido en sus pronunciamientos que la legalidad de una conducta no puede eximir a una empresa cuando una autoridad de competencia analiza ese comportamiento desde la perspectiva

[22] Véase el Caso B6-22/16. Abusive business terms due to inappropriate data processing, del Bundeskartellamt, párrafo 535.
[23] Véase el Caso B6-22/16. Abusive business terms due to inappropriate data processing, del Bundeskartellamt, párrafo 873.
[24] Caso 25-D-02. Practices implemented in the sector for mobile application advertising on iOS devices, párrafo 497, que cita Casos acumulados T-191/98, T-212/98 a T-214/98, Atlantic Container Line AB y otros contra Comisión de las Comunidades Europeas. ECLI:EU:T:2003:245, párrafo 1124; y Caso AT.40437, Apple – App Store Practices (music streaming). C(2024), párrafos 540-546.
[25] Caso T-136/19, Bulgarian Energy Holding y otros/Comisión. ECLI:EU:T:2023:669, párrafo 951.

de la aplicación de los artículos 101 y 102 del TFUE[26]. La clasificación legal de una conducta bajo una legislación distinta de la de defensa de la competencia no forma parte del análisis de la capacidad de la conducta para restringir el libre funcionamiento del mercado[27].

A diferencia de la normativa sectorial, la legislación en materia de protección de datos no se puede considerar automáticamente complementaria respecto de las normas de competencia. Los objetivos que persiguen son distintos. Según el TJUE ambas normas son distintas, sin seguir cursos paralelos. Por tanto, su aplicación debe realizarse de forma incidental por parte de aquellas autoridades que no sean competentes en su interpretación.

En todo caso, el análisis debe distinguir entre supuestos donde la empresa instrumentaliza el incumplimiento normativo para cometer infracciones de competencia (como en el caso *Facebook*) frente a meras coincidencias de infracciones en ambas disciplinas sin nexo causal.

La cooperación entre autoridades de competencia y protección de datos personales

Ni el RGPD ni ningún otro instrumento del Derecho de la Unión Europea establecen normas específicas relativas a la cooperación entre las autoridades de competencia y las autoridades de protección de datos.

El TJUE clarificó los pasos que debe seguir una autoridad de competencia cuando considere necesario pronunciarse, en el marco de una decisión relativa a la infracción de competencia, sobre la conformidad con el RGPD de un tratamiento de datos personales efectuado por una empresa[28].

El primero de estos pasos se refiere a la necesidad de la autoridad de pronunciarse en una materia ajena. No todo incumplimiento de la legislación de protección de datos es suficientemente relevante para alguno de sus procedimientos.

Una vez que la autoridad de competencia determine la necesidad de su intervención, el TJUE señala que las **autoridades de protección de datos y de competencia deben cooperar entre sí para garantizar una aplicación coherente de la legislación** de protección de datos personales[29].

De acuerdo con el principio de cooperación leal consagrada en el artículo 4.3 del Tratado de la Unión Europea, cuando la autoridad de competencia considere necesario apreciar la conformidad de la legislación de protección de datos personales para su propio análisis, está obligada a respetar las competencias de las autoridades de protección de datos. No obstante, ese principio no impone una obligación explícita de buscar un acuerdo común sobre su aplicación o interpretación. La autoridad de competencia debe comprobar si esa actividad o una actividad similar ya ha sido objeto de una

[26] Caso C-457/10 P, AstraZeneca AB y AstraZeneca plc contra Comisión Europea. ECLI:EU:C:2012:770, párrafo 132.
[27] Caso C-457/10 P, AstraZeneca AB y AstraZeneca plc contra Comisión Europea. ECLI:EU:C:2012:770, párrafos 74 y 132; Caso C-377/20, Servizio Elettrico Nazionale SpA y otros contra Autorità Garante della Concorrenza e del Mercato y otros. ECLI:EU:C:2021:998, párrafo 35.
[28] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 52.
[29] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 52. En este sentido, la ACCO y la Autoridad Catalana de Protección de Datos suscribieron un protocolo de colaboración en junio de 2024 con la finalidad de establecer un marco de colaboración conjunto. Véase https://dogc.gencat.cat/es/document-del-dogc/index.html?documentId=990320.

decisión por parte de una autoridad de protección de datos, o incluso por parte del propio Tribunal[30]. Esta consulta es preceptiva para la autoridad de competencia. Nada garantiza, sin embargo, que las autoridades de protección de datos respondan a las consultas antes de que la autoridad complete su investigación y sancione la conducta.

La autoridad de competencia puede cumplir con su obligación preceptiva de consultar a una autoridad de protección de datos al elegir una de ellas según el criterio que más le convenga para su propio análisis.

En caso de que la autoridad de protección de datos afirme que ese mismo supuesto de hecho ha sido objeto de una decisión, la autoridad de competencia no puede apartarse de sus pronunciamientos. La autoridad de competencia conserva su libertad para extraer sus propias conclusiones desde el punto de vista de la aplicación del Derecho de la competencia[31]. La autoridad de competencia deberá tener en cuenta si la autoridad de protección de datos ha declarado la conformidad de la conducta respecto de la legislación sobre la que es competente para considerarlo en el contexto económico y legal de esta, pero esta conclusión no será determinante para establecer la inexistencia de una infracción en materia de competencia. Si la autoridad de protección de datos no formula ninguna objeción al análisis de competencia, se podrá realizar ese análisis sin necesidad de esperar a la adopción de una decisión por su parte[32].

El TJUE impone la obligación a la autoridad de competencia y al resto de autoridades competentes de cooperar para que puedan determinar si, antes de iniciar su propia apreciación, no procede esperar a la adopción de una decisión por parte de la autoridad de protección de datos interesada[33]. Tendrá prioridad la autoridad de protección de datos en su pronunciamiento, ya que es la competente para realizar la interpretación y aplicación de esas normas. La autoridad de competencia deberá esperar a que la autoridad competente tome una decisión sobre el asunto y, en caso de que lo haga, no podrá distanciarse de sus conclusiones.

Si la autoridad de protección de datos no da respuesta a la autoridad de competencia en un plazo razonable a la solicitud de la autoridad de competencia o no coopera adecuadamente, esta podrá proseguir su propia investigación[34].

En todo caso, las autoridades de protección de datos deben comunicar toda la información de la que dispongan sobre el mismo supuesto de hecho para tratar de disipar sus dudas o, en su caso, deben informar a la autoridad de competencia de si tiene previsto activar el procedimiento de cooperación de conformidad con el RGPD[35].

[30] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 56.
[31] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 56.
[32] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 59.
[33] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 57.
[34] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 57.
[35] Véase el Caso C-252/21, Meta Platforms Inc. y otros contra Bundeskartellamt. ECLI:EU:C:2023:537, párrafo 58.

4. Recomendaciones

En materia de cooperación con las autoridades de protección de datos personales

Por lo que respecta a la cooperación, la autoridad de competencia puede cumplir con su obligación preceptiva de consultar a una autoridad de protección de datos escogiendo una de las competentes por razón de la materia o del territorio, según el criterio que más le convenga para su propio análisis. No obstante, debería comprobar las actividades y decisiones tanto de la autoridad de protección de datos personales de su mismo Estado miembro como, si procede, de otros. Es posible que la autoridad de un mismo Estado miembro no haya analizado la misma conducta porque simplemente no es la autoridad competente para hacerlo (la autoridad de control principal), de acuerdo con las disposiciones del RGPD. En este caso, debería tratar de ponerse en contacto, al menos, con la autoridad de control principal dependiendo del establecimiento europeo que tenga el responsable del tratamiento, así como la autoridad de protección de datos de su mismo Estado miembro, con el fin de que pueda facilitarle información adicional sobre posibles actividades en otros Estados miembros.

Cuando ninguna autoridad de protección de datos haya emitido una decisión al respecto, pero conozca del asunto ejerciendo las competencias que le son propias, la autoridad de competencia no está vinculada por ninguna decisión, sino que debe consultar y solicitar su cooperación a las autoridades que contacte para decidir si sería deseable que esperase a adoptar su propia decisión después de la autoridad de protección de datos.

Idealmente, esta consulta debiera realizarse por la autoridad de competencia cuando se encuentre en una fase preliminar (antes de iniciar la fase de instrucción) para determinar el valor añadido y los bienes jurídicos distintos que se protegerían mediante un procedimiento adicional en materia de competencia. Las autoridades de protección de datos pueden formular objeciones a que la investigación de la autoridad de competencia prosiga en ese momento.

En todo caso, las autoridades de competencia deben demostrar que han accionado estos mecanismos para tratar de recabar una respuesta por parte de las autoridades de protección de datos. En caso de que no la reciban, nada obsta para que prosigan su investigación. La incomparecencia de las autoridades de protección de datos no justifica que las autoridades de competencia abandonen su deber de observar el contexto económico y legal de la conducta.

En materia del análisis de competencia

Una infracción de competencia no se puede derivar directamente de una infracción en materia de protección de datos personales. Este elemento es únicamente un indicador útil que puede servir a una autoridad de competencia, por ejemplo, para establecer que existe un abuso de posición dominante en un determinado mercado. Implícitamente, esto comporta que a este elemento deben sumarse

muchos más, que observen la propia conducta en cuestión y su capacidad para restringir la competencia en mercados adyacentes o aguas abajo. En abstracto, se necesita algo más que aseverar que se ha dado un incumplimiento del RGPD para equipararlo a una infracción de competencia, sin perjuicio de que algunas autoridades de competencia han seguido este camino.

Esta premisa no obsta a que una autoridad de competencia establezca que la infracción del RGPD es el efecto anticompetitivo que se genera como consecuencia de la existencia de la infracción de las normas de competencia. En este caso, ambas infracciones se encontrarían íntimamente relacionadas y resultaría muy complejo desligar una de otra, por lo que la autoridad de competencia debiera identificar de forma clara los bienes jurídicos que está protegiendo.

Por último, la protección de datos personales no debe considerarse únicamente como un parámetro de competencia, a la altura de otros tradicionalmente considerados como el precio o la calidad de un bien o servicio, sino como una manifestación clara de la libertad de elección de la que disponen los consumidores, que también debe protegerse mediante las normas de competencia. Cuanto mayor sea la capacidad de un consumidor de elegir entre un tratamiento intensivo o liviano de sus datos personales para la prestación de un servicio digital, mayores incentivos existirán, por tanto, para los operadores de estos mismos servicios para tender hacia unos modelos de negocio garantes de los derechos fundamentales de sus usuarios.

Para las autoridades de competencia

De conformidad con el estudio encargado por la ACCO, las **recomendaciones** para las autoridades de competencia, en lo que respecta a la interacción entre la defensa de la competencia y la protección de los datos personales, son las siguientes:

- **Reconocer la doble naturaleza de los datos:** entender que los datos personales son a la vez un activo económico y un derecho fundamental, y su uso indebido puede distorsionar mercados y afectar derechos.

- **Integrar la protección de datos personales en el análisis competitivo**, como parámetro de calidad, al mismo nivel que el precio, la innovación o la variedad en el mercado.

- **Coordinación con las autoridades de protección de datos:** establecer canales formales y tempranos de cooperación, siguiendo el principio de cooperación leal, para evitar contradicciones y reforzar la efectividad regulatoria.

- **No paralizar investigaciones por falta de cooperación:** si la autoridad de protección de datos no responde a tiempo, continuar con el análisis en competencia para no debilitar la tutela de los mercados.

- **Respetar la interpretación del RGPD:** tomar en cuenta las decisiones jurídicas de las autoridades competentes en protección de datos, aunque se puedan derivar consecuencias diferentes en clave de competencia.

- **Atender a los riesgos de acumulación y acceso a datos:** analizar si la concentración exclusiva de grandes volúmenes de datos constituye una barrera de entrada o limita la innovación en mercados digitales.

- **Evaluar la forma en la que se presta consentimiento como posible abuso:** el consentimiento impuesto puede constituir una explotación abusiva.

- **Construir teorías del daño sólidas:** evitar equipar automáticamente la infracción del RGPD con infracción de competencia y usarla como indicio que debe integrarse en un análisis más amplio.

- **Apoyar la portabilidad de datos y el principio de minimización:** impulsar la portabilidad de datos como remedio procompetitivo y valorar si el uso excesivo de datos constituye un mecanismo de exclusión.

- **Adoptar un enfoque dinámico y multidisciplinar:** promover la formación cruzada en competencia y protección de datos, y anticipar riesgos emergentes con una visión prospectiva de los mercados digitales.

Autoritat Catalana
de la Competència
Via Laietana, 60 - 08003 Barcelona
Tel.: 93 552 81 60
autoritat.competencia@gencat.cat
http://acco.gencat.cat
@competenciacat

ACCO Autoritat Catalana de la Competència

Generalitat de Catalunya