



DAVID VS. GOLIAT: LAS OBLIGACIONES DE TRANSPARENCIA EN EL USO DE DATOS POR LOS “GUARDIANES DE ACCESO” EN LA LEY DE MERCADOS DIGITALES

DAVID VS. GOLIATH: TRANSPARENCY OBLIGATIONS ON THE USE OF DATA BY “GATEKEEPERS” IN THE DIGITAL MARKETS ACT

MARGARITA OROZCO GONZÁLEZ

Profesora Contratada Doctora de Derecho Civil
Universidad de Murcia

Revista Aranzadi Doctrinal 5 • Mayo 2023 • Págs. 29 a 46

Fecha de recepción: 17-3-2023

Fecha de aceptación: 27-3-2023

Resumen: El gran peso que han alcanzado algunos prestadores de servicios en el mercado digital europeo ha determinado el surgimiento de determinadas barreras de acceso al mismo, que amenazan la libre competencia, al permitirles ocupar una posición hegemónica que frena la entrada de nuevos competidores, así como limitar las posibilidades de expansión de aquellos ya existentes. Especial relevancia posee, en este contexto, la enorme ventaja competitiva que les aporta el gran volumen de datos que tratan, dado el elevado número de usuarios que poseen, lo que les permite perfeccionar su servicio y personalizarlo, haciendo uso de las técnicas que ofrecen el Big Data y la Inteligencia Artificial. Al fin de solucionar tal problemática,

Abstract: The great weight of some service providers in the European digital market has led to the emergence of certain barriers to access, which threaten free competition, by allowing them to occupy a hegemonic position that hinders the entry of new competitors, as well as limiting the possibilities of expansion of existing ones. Particularly relevant in this context is the enormous competitive advantage provided by the large volume of data they process, given the large number of users they have, which allows them to perfect their service and personalize it, making use of the techniques offered by Big Data and Artificial Intelligence. In order to solve this problem, the European legislator has approved a regulatory package, of which we

el legislador europeo ha aprobado un paquete normativo, del que cabe destacar la Ley/Reglamento de Mercados Digitales, que crea la figura de los “Guardianes de Acceso”, imponiéndoles unas obligaciones específicas, entre las que se pueden subrayar las relativas a la transparencia y limitación del tratamiento de datos.

Palabras clave: Ley Mercados Digitales – Plataformas de servicios digitales – Protección de datos – Transparencia – Guardianes de acceso – Obligaciones – Servicios básicos de plataforma.

should highlight the Law/Regulation of Digital Markets, which creates the figure of the “Access Guardians” or “Gatekeepers”, imposing specific obligations on them, among which those relating to the transparency and limitation of data processing can be highlighted.

Keywords: Digital Markets Act – Digital services platforms – Data protection – Transparency – Gatekeepers – Obligations – Core platform services.

SUMARIO

I. EL ESTADO DE LA CUESTIÓN. II. BREVE ANÁLISIS DE LA LEY DE MERCADOS DIGITALES EUROPEA. 1. *Su ámbito objetivo: los “Gatekeepers” o “Guardianes de acceso” y su posición aventajada.* 2. *Obligaciones específicas de los guardianes respecto al acceso y utilización de datos personales.* 3. *Otras obligaciones relacionadas: auditoría y comprobación y responsabilidad.* III. APUNTES FINALES. IV. BIBLIOGRAFÍA.

I. EL ESTADO DE LA CUESTIÓN

El Mercado de servicios digitales actual se caracteriza por la oferta de un amplísimo abanico de servicios, prestado por un elevado número de empresas, de diverso tamaño o entidad y arraigo. Esos servicios, como refleja el Informe de la Comisión Europea “Sector inquiry into consumer Internet of Things” de 21 de enero de 2022¹, tienen una creciente presencia en la vida diaria de los ciudadanos/consumidores. A nadie resulta ya ajeno, a día de hoy, la omnipresente inmersión de las nuevas tecnologías en la vida de cualquier ciudadano. Así, el uso intensivo y extensivo de Internet y los servicios ofrecidos a través de dicho canal es la vía habitual por la que, actualmente, nos relacionamos con nuestro entorno personal y profesional –por ejemplo, a través de servicios de mensajería como WhatsApp o Telegram, o haciendo uso de redes sociales como Instagram, Facebook, TikTok, etc., o bien vía correo electrónico, servicio ofrecido por empresas como Google, Msn, etc.– y adquirimos bienes y servicios. Es más, el propio acceso a los servicios

1. REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT, “Final report – sector inquiry into consumer Internet of Things”, COM (2022) 19 final, 20/01/2022. Fuente: https://competition-policy.ec.europa.eu/system/files/2022-01/internet-of-things_final_report_2022_en.pdf.

antes mencionados, creando el pertinente perfil, ya supone una contratación electrónica, al igual que sucede con las compras por Internet de todo tipo de productos, canal de contratación cada vez más extendido en nuestra sociedad del Siglo XXI.

Las cifras demuestran que las ventas mundiales de comercio electrónico alcanzaron los 26,7 billones de dólares a nivel global en 2019, lo que supone un crecimiento del 4% con respecto a 2018, según destaca la UNCTAD en su informe “UNCTAD Technical Notes on ICT for Development”, de 2021². En cuanto al volumen de usuarios, gracias a la información que han ido remitiendo recientemente las plataformas para empezar a dar cumplimiento al nuevo marco regulatorio europeo del mercado único digital, configurado por los Reglamentos de Mercados digitales y el de Servicios digitales –para lo que tenían de plazo hasta el 17 de febrero de 2023–, se sabe que YouTube cuenta con 401,7 millones de usuarios mensuales activos en Europa, mientras que Facebook posee 255 millones de usuarios europeos, Instagram 250 millones y TikTok cuenta con 125 millones de usuarios en el territorio de la UE³.

Siguiendo esta línea, nos encontramos con que, en el citado informe sobre IoT, los participantes respondieron masivamente identificando como algunas de las principales barreras de acceso a estos servicios, de manera somera, de un lado, los problemas relativos a la falta de interoperabilidad, de otro, la imposibilidad de competir con los grandes prestadores de servicios y, también, la falta de acceso a los datos.

Dentro de estos problemas, el relativo a la existencia de empresas de gran tamaño y presencia estable y duradera en el mercado digital europeo nos sitúa en un escenario en el que las pequeñas y medianas plataformas, prestadoras de servicios de la sociedad de la información, se equiparan a la figura de David del relato bíblico, teniendo que enfrentarse al gigante Goliat. Sin embargo, en este escenario real actual las posibilidades del pequeño prestador de vencer al gigante son francamente menores, casi nulas, dadas las ventajas que la posición aventajada de este le proporciona.

El legislador europeo, siendo cada vez más consciente de esta problemática, ha buscado desarrollar un marco normativo que estructure este mercado y equilibre las condiciones en la prestación de estos servicios. Se trata del Reglamento (UE) 2022/1925, que regula los mercados en el sector digital, conocido como Ley de mercados digitales (LDM), o por sus siglas en inglés DMA, que proceden de *Digital Markets Act*. El texto normativo fue publicado en el Diario Oficial el 12 de

2. UNCTAD “Technical Notes on ICT for Development. ESTIMATES OF GLOBAL E-COMMERCE 2019 AND PRELIMINARY ASSESSMENT OF COVID-19 IMPACT ON ONLINE RETAIL 2020”, publicado en 2021.

3. Al respecto, *vid.* <https://www.xataka.com/legislacion-y-derechos/hoy-era-limite-tecnologicas-revelaran-cuantos-usuarios-tienen-europa-al-fin-conocemos-su-poder-real>. <https://www.elblogsalmon.com/economia/facebook-instagram-youtube-tiktok-este-numero-usuarios-principales-plataformas-europa>.

octubre de 2022, entrando en vigor el día 1 de noviembre de 2022, aunque no comenzará a aplicarse hasta transcurridos seis meses de dicha fecha, por tanto, de forma inminente a partir del 2 de mayo de 2023.

Dicha norma, como analizaremos con más en detalle a continuación, tiene como destinatario directo a esas grandes plataformas. Así, como se constata en la LDM, el mercado digital está configurado por una multiplicidad de empresas-prestadores de servicio de muy diversa entidad, pero se evidencia la existencia de un reducido número de ellos que, por su tamaño, ejercen una suerte de, si no monopolio, sí posición hegemónica: son los denominados por la nueva normativa Europea “Gatekeepers” o “Guardianes de Acceso”.

En relación al precitado texto legal europeo, articula una regulación de control estricto del funcionamiento y actuación de dichas grandes plataformas, tanto en lo que afecta a sus usuarios finales – particulares – cuanto en lo referente a sus usuarios profesionales –aquellas empresas o prestadores que se valen de los servicios del guardián de acceso para llegar a sus potenciales clientes o realizar la oferta de sus servicios–, buscando, en todo caso, establecer unas reglas de mercado abierto que fomente la competencia. Asimismo, y persiguiendo tal fin, estructura unas normas protectoras de los datos de carácter personal, a la vez que facilita y garantiza el ejercicio de determinados derechos consagrados en el Reglamento General de Protección de datos (RGPD), a través del establecimiento de determinadas obligaciones de transparencia, rendición de cuentas y supervisión.

II. BREVE ANÁLISIS DE LA LEY DE MERCADOS DIGITALES EUROPEA

Como ya hemos tenido ocasión de subrayar anteriormente, la LDM tiene por objeto evitar que los guardianes de acceso impongan condiciones injustas a las empresas y los usuarios finales, así como garantizar el carácter abierto de estas grandes plataformas o conglomerados de empresas prestadoras de este tipo de servicios.

Para ello, el objetivo principal del legislador europeo es determinar qué prestadores deben quedar recogidos dentro de esta categoría.

1. SU ÁMBITO OBJETIVO: LOS “GATEKEEPERS” O “GUARDIANES DE ACCESO” Y SU POSICIÓN AVENTAJADA

Respondiendo al objetivo señalado consistente en reducir las barreras existentes en el mercado único digital con la configuración de un ecosistema de servicios prestados en un contexto de igualdad, de competencia leal y en el que sea posible el acceso al mercado sin afrontar un bloqueo casi absoluto, derivado de las barreras impuestas por las grandes empresas del sector, la norma se centra en las grandes plataformas de servicios en línea a las que se les ha dado en denominar

“Gatekeepers” o “Guardianes de acceso”. Para ser categorizadas como tales, las plataformas en cuestión deben de cumplir una serie de requisitos que se determinan en el texto.

Como premisa para la posterior concreción de qué servicios en línea colman tal concepto, hemos de analizar la definición de la noción de plataforma, la cual, sorprendentemente, no se contempla en la LMD. Así, como primer escollo, hemos de afrontar el hecho de que, a día de hoy, no existe un concepto normativo, tal y como ha subrayado la doctrina especializada⁴, aunque, como destaca ÁLVAREZ MORENO⁵, sí que ha habido intentos de clarificación de esta noción por algunos documentos, como es el caso de la Comunicación de la Comisión Europea “Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy”, en el año 2015, aunque no ha sido hasta la aprobación del, Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022, relativo a un mercado único de servicios digitales, más conocido como Reglamento Europeo de Servicios digitales (en adelante, LSD) – que configura el paquete normativo, junto a la LMD, desarrollado la UE para regular este mercado de servicios – cuando se ha logrado una definición aportada por el legislador. En tal sentido, de acuerdo con el art. 3, apartado i) LSD, se ha de entender por plataforma aquel *“servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento”*.

Partiendo de la base de esta noción y volviendo a la LMD, la referencia que se hace al ámbito subjetivo de la norma en el art. 1.2. se refiere a “servicios básicos de plataforma” ofertados por guardianes de acceso a usuarios profesionales y finales, situados en el territorio de la UE, independientemente de donde tengan situado su lugar de establecimiento o residencia⁶. Desgranando el concepto legal, nos encontramos con que solo las plataformas prestadoras de los considerados “servicios básicos de plataforma” que sean clasificadas como guardianes de acceso, serán las compelidas a cumplir con los mandatos y previsiones contenidos en la norma. Para identificar cuáles son, hemos de acudir al articulado de la misma,

4. Así, por ejemplo, *vid.* VILALTA NICUESA, A. E., “La regulación europea de las plataformas digitales en la era de la economía colaborativa”, *RCDI*, núm. 765, 2018.

5. *Vid.* ÁLVAREZ MORENO, La contratación electrónica mediante plataformas en línea: modelo negocial (B2C), Editorial Reus, 2021; p. 20 y ss.

6. Con ello, como destaca MADRID PARRA, “Son los servicios de plataforma en línea el gran punto de conexión entre los dos Reglamentos que forma un mismo paquete regulador del sector digital del mercado. La plataforma en línea se convierte en el gran sistema de soporte tecnológico que permite prestar el conjunto de servicios digitales”. (MADRID PARRA, A., “Aproximación inicial a los Reglamentos Europeos sobre servicios y mercados digitales”, *La Ley Unión Europea*, núm. 110, enero 2023; p. 13.

buscando la determinación de qué servicios integran esta lista, así como los criterios marcados por el legislador para concretar qué plataformas son consideradas “guardianes de acceso”.

En cuanto a la primera de las incógnitas, nos es resuelta por el artículo 2.2 LMD, donde se especifica que se consideran “servicios básicos de plataforma” los: “a) servicios de intermediación en línea; b) motores de búsqueda en línea; c) servicios de redes sociales en línea; d) servicios de plataforma de intercambio de videos; e) servicios de comunicaciones interpersonales independientes de la numeración; f) sistemas operativos; g) navegadores web; h) asistentes virtuales; i) servicios de computación en nube; y j) servicios de publicidad en línea, incluidas las redes de publicidad, las plataformas de intercambio de publicidad y cualquier otro servicio de intermediación publicitaria, prestados por una empresa que preste cualquiera de los servicios básicos de plataforma enumerados en las letras a) a i)”. Por tanto, como primer paso para ser categorizada como “gatekeeper”, la plataforma debe prestar, al menos, uno de estos servicios. Entendemos que se trata de una lista tasada, basándonos en la terminología empleada en la redacción y en el hecho de que no se incluye ninguna previsión que permita concluir una posible aplicación analógica o extensiva de lo recogido. En todo caso, además, coincidimos con MORALES BARCELÓ en que, en la práctica, la designación de estos servicios no será sencilla, por cuanto “a pesar de que el artículo 2 de la PRMD, recoge una serie de definiciones, hay una remisión a otras normas en lo relativo a los servicios prestados”⁷, lo que complicará la tarea interpretativa, al poder generar cierta indefinición.

Partiendo de esta premisa previa, el artículo 3, apartado 1, nos ofrece las pautas para clasificar a dichos prestadores, indicando que se consideran como tales aquellas empresas que desempeñan –o es previsible que lo hagan– un papel especialmente importante en el mercado interior, gozando de una posición arraigada y duradera en éste, sirviendo de puente de enlace entre sus usuarios profesionales y los potenciales clientes de éstos, usuarios finales de la plataforma. Como se subraya en el documento de la Comisión Europea, de 31 de octubre de 2022 (QANDA/20/2349): “Preguntas y respuestas: Ley de Mercados Digitales: garantizar unos mercados digitales justos y abiertos”, se tratan de tres requisitos acumulativos, siendo preciso, en principio, que se cumplan los tres para que el servicio pueda ser considerado “gatekeeper”.

Con el fin de disponer de criterios objetivos para evaluar el cumplimiento de los citados requisitos, el apartado 2 del art. 3 establece unas pautas cuantitativas para cada uno de los tres, que, de alcanzarse en la práctica, configuran una presunción de cumplimiento del requisito en cuestión, la cual se debe considerar

7. MORALES BARCELÓ, J., “Los guardianes de acceso y la dudosa necesidad de la propuesta de ley de mercados digitales: especial referencia a las concentraciones económicas”, *Revista de Derecho de la Competencia y la Distribución*, núm. 28, Sección Estudios, 2021, Wolters Kluwer; p. 3.

iuris tantum, de acuerdo con la previsión contenida en el apartado 5 del mismo precepto. Conforme a éste, pese a la suposición de que las plataformas que reúnen los anteriores requisitos serán consideradas “guardianes de acceso”, se les reconoce la posibilidad de refutar dicha presunción, aportando una argumentación fundada que demuestre que, por circunstancias excepcionales, no debe ser categorizada como tal⁸.

Teniendo presente esa precisión, los criterios ponderativos mencionados son los siguientes. En primer lugar, respecto al requisito de que la empresa ostente una posición de influencia en el mercado, se considerará colmado cuando *“la empresa consiga un volumen de negocios anual en la Unión igual o superior a 7 500 000 000 EUR en cada uno de los tres últimos ejercicios, o cuando su capitalización bursátil media o su valor justo de mercado equivalente ascienda como mínimo a 75 000 000 000 EUR en el último ejercicio, y preste el mismo servicio básico de plataforma en al menos tres Estados miembros”*. Por otro lado, y en segundo lugar, en lo atinente al requisito de que la empresa constituya una importante pasarela de conexión entre los usuarios profesionales y los finales, se entenderá cumplido cuando *“proporcione un servicio básico de plataforma que, en el último ejercicio, haya tenido al menos 45 millones mensuales de usuarios finales activos establecidos o situados en la Unión y al menos 10000 usuarios profesionales activos anuales establecidos en la Unión, identificados y calculados de conformidad con la metodología y los indicadores establecidos en el anexo”*. Por último, en cuanto a la exigencia de que la plataforma posea una posición duradera y arraigada, o lo vaya a hacer en un futuro próximo, se considerará cumplida cuando *“hayan alcanzado los umbrales establecidos en la letra b) del presente apartado en cada uno de los últimos tres ejercicios”*.

En todo caso, la norma contempla una suerte de *carte blanche* para la Comisión, al reconocer el apartado 8 del artículo 3 la posibilidad de que ésta designe como “guardián de acceso” a *“cualquier empresa prestadora de servicios básicos de plataforma que cumpla todos los requisitos del apartado 1 del presente artículo, pero no alcance todos los umbrales establecidos en el apartado 2 del presente artículo”*; lo que, a nuestro juicio, contribuye a la creación de cierta inseguridad jurídica en el mercado, al reconocer que, incluso no cumpliendo las pautas exigidas, es posible la inclusión dentro de esta nueva categoría de grandes plataformas, evaluando otras cualidades o características⁹,

8. Art. 3 apartado 5 LMD “La empresa prestadora de servicios básicos de plataforma podrá presentar, junto con su notificación, argumentos suficientemente fundamentados para demostrar que, excepcionalmente, pese a haber alcanzado todos los umbrales establecidos en el apartado 2, dadas las circunstancias en las que opera el servicio básico de plataforma de que se trate, no cumple los requisitos enumerados en el apartado 1”.

9. Al respecto, el citado precepto, dispone que “A tal fin, la Comisión tendrá en cuenta algunos de los elementos siguientes, o todos ellos, en la medida en que sean pertinentes para la empresa prestadora de servicios básicos de plataforma de que se trate:

a) el tamaño, incluidos el volumen de negocios y la capitalización bursátil, las operaciones y la posición de dicha empresa;

que consideramos en exceso inconcretas, sobre todo la contenida en el apartado g), que hace referencia a cualesquiera “otras características estructurales de las empresas o servicios”, términos que adolecen de una notable carga de imprecisión e inconcreción.

Con todo, el procedimiento para la calificación como guardián de acceso a la plataforma está previsto, por un lado, en el artículo 3 y, por otro, en el art. 17. Así, en primer lugar, ex art. 3.3., será la propia empresa, una vez que constate el cumplimiento de los requisitos mencionados, quien deba comunicar tal extremo a la Comisión, teniendo como plazo máximo para ello los dos meses siguientes a la consecución de los umbrales establecidos. Si se confirma que reúne los requisitos, de acuerdo con el art. 3.4, *“La Comisión designará como guardián de acceso, sin demora indebida y a más tardar 45 días hábiles después de recibir la información completa a que se refiere el apartado 3, a una empresa prestadora de servicios básicos de plataforma que alcance todos los umbrales establecidos en el apartado 2”*; asimismo, si la plataforma ha ejercitado la potestad de oposición reconocida en el apartado 5, pero la Comisión no considera suficientemente fundada su argumentación, según lo dispuesto en el ap. 5 párr. 4.º, podrá designarla como tal de manera unilateral.

Por otro lado, el artículo 17 contempla una vía de designación como “guardián de acceso” que se basa en la investigación del mercado por parte de la Comisión Europea, lo que la habilita a examinar su situación y características para proponer su eventual clasificación, emitiendo una “decisión de designación”, mediante un acto de ejecución, de acuerdo con lo regulado en el art. 50.2.

Aquellas plataformas que integran la categoría de “gatekeepers”, pertenecen a un pequeño y *selecto* grupo de grandes corporaciones con un enorme poder en el mercado, como consecuencia de las características antes mencionadas que reúnen en la práctica, y gozan de evidentes ventajas frente a la competencia; lo que, como subraya el Considerando 3 LMD, *“(…) les permite trasladar sus ventajas, como su acceso a grandes cantidades de datos, de un ámbito de actividad a otro”*.

b) el número de usuarios profesionales que utilizan el servicio básico de plataforma para llegar a los usuarios finales y el número de usuarios finales;

c) los efectos de red y las ventajas derivadas de los datos, en particular en relación con el acceso de dicha empresa a los datos personales y los datos no personales, con la recopilación de esos datos por parte de la empresa o con sus capacidades de análisis;

d) cualesquiera efectos relacionados con la escala o el alcance de los que se beneficie la empresa, en particular con respecto a los datos y, en su caso, a sus actividades fuera de la Unión;

e) la cautividad de los usuarios profesionales o finales, incluidos los costes que conlleva el cambio de empresa prestadora y los sesgos de comportamiento que reducen la capacidad de los usuarios profesionales y los usuarios finales para cambiar de empresa prestadora o recurrir a varias para un mismo servicio;

f) una estructura de conglomerado empresarial o una integración vertical de la empresa que, por ejemplo, le permita compensar ganancias y pérdidas entre actividades, combinar datos procedentes de distintas fuentes o aprovechar su posición, o

g) otras características estructurales de las empresas o servicios”.

Basándonos en lo anterior, conviene hacer especial hincapié en la gran relevancia que poseen los datos de carácter personal en la posición aventajada y hegemónica de dichas plataformas, tal y como reconoce nuestro legislador europeo. En efecto, el acceso a la información, con las posibilidades de tratamiento que facilitan hoy en día las técnicas de Big Data e Inteligencia Artificial, posibilitando un perfilado de gran precisión de cada usuario, constituye un activo clave de estas grandes empresas.

2. OBLIGACIONES ESPECÍFICAS DE LOS GUARDIANES RESPECTO AL ACCESO Y UTILIZACIÓN DE DATOS PERSONALES

Como hemos subrayado, una de las principales preocupaciones subyacentes en la norma que nos ocupa es el amplio volumen de datos a los que tiene acceso un “gatekeeper”, que le permite personalizar su servicio y la publicidad del mismo de un modo inalcanzable para los pequeños prestadores, en concreto sus usuarios profesionales, lo que le posibilita, además, valerse de esa ventaja competitiva para recabar aún más información de sus usuarios finales. Con ello en mente, el Considerando 36 LMD impone que para garantizar que los guardianes de acceso 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 de tratamiento de datos e inicio de sesión 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. Ello, no obstante, cabe reseñar, se basa en el mandato contenido en el Reglamento Europeo General de Protección de Datos, de 2016 (RGPD).

Para configurar esta tutela de los datos en el contexto de los servicios básicos de plataforma, la LMD contempla una definición de dato en su art. 2 apartado 24, según el cual lo será *“cualquier representación digital de actos, hechos o información y cualquier compilación de tales actos, hechos o información, también en forma de grabación sonora, visual o audiovisual”* Ese concepto, en todo caso, se debe entender como complementario de aquel amplio, recogido en el art. 4 RGPD, que, nos permitimos recordar, entiende por dato personal *–“ 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”*–, lo que abarca tanto el concepto amplio de dato personal, cuanto el más restrictivo y blindado de dato sensible.

En este orden de ideas, las obligaciones *extra* que contempla la LMD en este contexto parten de las actuales reglas marcadas por el RGPD para el acceso y

tratamiento de información personal. Así, tengamos presente que dicha regulación, de forma novedosa con respecto a la Directiva que le precedía, instituyó la obligación de recabar el consentimiento expreso, específico e individualizado para cada tratamiento, libre, informado e inequívoco¹⁰, haciendo desaparecer la opción de la presunción de su existencia con el establecimiento de casillas pre-marcadas. Además, como ya se destacaba en el precitado Reglamento de Protección de Datos (en concreto, en su art. 7), en los Considerandos de la LMD se hace especial hincapié en que debe ser igual de sencillo para el usuario retirar su consentimiento, o modificarlo, que darlo en primer lugar.

Unido a lo anterior, se configura una obligación de información que va más allá de lo previsto en el RGPD: el deber de informar acerca de la libertad que tiene el usuario de los servicios básicos de plataforma para no consentir el tratamiento de su información –en concreto, aquellos datos no indispensables para la prestación–, sin que ello suponga la imposibilidad de acceder al servicio y sin que ello pueda implicar, en principio, una pérdida de calidad de éste– esto último, con algunos matices que analizaremos a continuación. Consideramos la inclusión de este mandato un total acierto del legislador, pero, por otra parte, albergamos serias dudas acerca de su carácter imperativo ya que, de la lectura del texto, no se puede concluir la inclusión de tal obligación en ninguno de sus preceptos y, como hemos tenido ocasión de subrayar en trabajos anteriores¹¹, existe un parecer mayoritario en la doctrina respecto al carácter no vinculante de los Considerandos de las normas europeas.

Así, el mentado Considerando 37 establece que *“en el momento de prestar el consentimiento, y solo cuando proceda, debe informarse al usuario final de que el hecho de no prestar el consentimiento puede dar lugar a una oferta menos personalizada, pero que, por lo demás, el servicio básico de plataforma va a permanecer inalterado y no se va a suprimir ninguna funcionalidad”*. La realidad que subyace a esta disposición reside en que las grandes plataformas, mediante el acceso a elevados volúmenes de datos que, además, pueden complementar con aquellos obtenidos en otros servicios ofrecidos en otras plataformas vinculadas, o los que

10. Como determina el Considerando 21 RGPD “El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal”, lo que se desarrolla en el art.7. El mismo espíritu lo encontramos presente en el Considerando 37 LMD, cuando dispone que “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”.

11. OROZCO GONZALEZ, M., “La utilización ilícita de datos de carácter personal por los partidos políticos”, Actualidad civil, núm. 7, 2021. Aquí ya sosteníamos que “Como punto de partida, debemos señalar que existe cierto debate en la doctrina acerca de la vinculación que los considerandos de un Reglamento europeo puedan tener para los Estados miembros, ya que una parte de la misma sostiene que son meros elementos interpretativos y, otros, que si implican una sujeción para el legislador nacional; cuestión que no es baladí en un supuesto como este, en el que, además, el partido político que presentó la enmienda que introdujo dicha posibilidad en la norma española lo justificó con la «obligatoriedad» que imponía el Considerando” (p. 5).

les aportan terceros, pueden ofrecer una alternativa más personalizada y, por ende, más enriquecida, a aquellos usuarios finales que consientan el tratamiento de su información de manera amplia. En tal caso, como destaca el Considerando 36 LMD, de ello *“se derivan ventajas similares de la práctica de i) combinar datos personales de usuarios finales recogidos de un servicio básico de plataforma con datos recogidos de otros servicios, ii) utilizar datos personales de un servicio básico de plataforma en otros servicios prestados por separado por el guardián de acceso, en particular servicios que no se prestan junto con el servicio básico de plataforma pertinente o en apoyo de este, y viceversa, o iii) iniciar la sesión de usuarios finales en diferentes servicios de guardianes de acceso para combinar datos personales”*. Esto contribuye innegablemente a bloquear la libre competencia en el mercado y el acceso al mismo, frente a lo cual la norma conmina a que, a modo de garantía, deban dar la libertad al usuario final de optar por aceptar tal personalización, prestando el consentimiento – en las condiciones ya mencionadas – para el acceso al servicio personalizado, o bien, no hacerlo y poder acceder a 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”*. (Considerando 36 LMD). En todo caso, esa versión del servicio menos individualizada, tal como destaca la Comisión en su informe de *“Preguntas y respuestas”*, ya mencionado *ut supra*, no debe ser diferente ni tener una calidad degradada en comparación con el servicio prestado a los usuarios finales que prestan su consentimiento¹².

No obstante, la previsión legal reconoce una excepción que habilita a que exista una merma en la calidad en aquellos supuestos en los que tal degradación *“sea consecuencia directa del hecho de que el guardián de acceso no pueda tratar dichos datos personales ni iniciar la sesión de los usuarios finales en un servicio”*. (Considerando 37), algo obvio en la práctica, puesto que es evidente que algunas funcionalidades pueden estar menos perfeccionadas de no ser posible la definición de un perfil – más o menos – exacto del usuario.

De manera específica, las obligaciones impuestas a estos prestadores están recogidas en los artículos 5, 6 y 7 LMD.

De entre ellas, nos vamos a centrar en aquellas que afectan o hacen referencia al tratamiento de datos, en concreto, los relativos a los usuarios finales.

En primer lugar, nos centramos en la prevista en el apartado 2 del artículo 5, referida a la transparencia en el tratamiento de la información. Así, se le impone, en primer término, al guardián de acceso que se abstenga de utilizar datos de usuarios finales que accedan a su plataforma para utilizar servicios de terceros (usuarios profesionales de la plataforma), con el fin de remitirles publicidad. En

12. Comisión Europea, de 31 de octubre de 2022, QANDA/20/2349, *“Preguntas y respuestas: Ley de Mercados Digitales: garantizar unos mercados digitales justos y abiertos”*, *op. cit.*

segundo lugar, se le prohíbe combinar datos obtenidos de la prestación de su servicio básico, procedentes de otros servicios del mismo tipo adicionales al principal o de cualquier otro servicio que proporcione el guardián de acceso, así como con datos personales procedentes de servicios de terceros. En tercer lugar, se le veta el cruce de los datos obtenidos en la prestación de ese servicio en cuestión con los recabados en otros servicios que proporcione el guardián de acceso por separado; y, por último, se le prohíbe iniciar la sesión de usuarios finales en otros servicios del guardián de acceso para combinar datos personales. Todo ello, por supuesto, siempre que el usuario final no haya prestado su consentimiento a tal fin, de la manera y con los requerimientos que establece el RGPD, en concreto, los establecidos en los artículos 4.11 y 7 RGPD. Asimismo, tal prohibición queda sin efecto en los casos en que, no mediando consentimiento expreso del usuario, el tratamiento quede legitimado por la presencia de alguna de las bases habilitantes que recoge el artículo 6, apartado 1, letras c), d) y e), del RGPD¹³.

Por su parte, el artículo 6 contempla una serie de obligaciones que, como reza su propio título, pueden ser desarrolladas a posteriori¹⁴. En el marco de la temática que nos ocupa, la primera obligación que recoge el precepto, en relación con el tratamiento de datos personales, la encontramos en el apartado 2, y es aquella que le conmina a no utilizar ninguna información, que no sea de acceso público¹⁵, proporcionada por sus usuarios profesionales en el uso de los servicios ofertados por la plataforma, en competencia con éste, así como los generados o aportados por los clientes de dichos usuarios profesionales.

Otras de las previsiones en este sentido, se recoge en el art. 6. 3, párrafo segundo, donde se impone que el guardián de acceso debe facilitar al usuario la posibilidad de cambiar, de modo sencillo, la configuración por defecto del sistema operativo cuando éste conduzca al usuario a publicidad de la plataforma. En todo caso, consideramos que la norma peca aquí de exceso de laxitud, por

13. Los supuestos en que, respectivamente: “el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”.

14. Ello se podrá producir en los supuestos previstos en el artículo 8 LMD, así como, según lo contemplado en el art. 12.1, en los casos en que “la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 49 por los que se complete el presente Reglamento respecto a las obligaciones establecidas en los artículos 5 y 6. Estos actos delegados se basarán en una investigación de mercado con arreglo al artículo 19 que haya determinado la necesidad de actualizar dichas obligaciones para hacer frente a las prácticas que limitan la disputabilidad de los servicios básicos de plataforma o que son desleales de la misma manera que las prácticas a que se refieren las obligaciones establecidas en los artículos 5 y 6”.

15. Esta característica la precisa en mayor detalle el párrafo segundo del citado apartado, donde se especifica que “A los efectos del párrafo primero, los datos que no sean públicamente accesibles incluirán todos los datos agregados y desagregados generados por los usuarios profesionales que puedan inferirse o recopilarse a través de las actividades comerciales de los usuarios profesionales o sus usuarios finales, entre ellos los datos sobre los clics, las búsquedas, las visualizaciones y la voz, en los servicios básicos de plataforma pertinentes o en los servicios prestados junto con los servicios básicos de plataforma del guardián de acceso pertinentes, o en apoyo de tales servicios”.

cuanto el RGPD exige que en el diseño de los productos – y un sistema operativo queda subsumido en dicho ámbito– se debe contemplar los principios de privacidad “por defecto” y “desde el diseño”; así las cosas, se debería haber extendido la exigibilidad de la observación de los mismos en el diseño de la propia plataforma, de modo que se garantice que, en ningún caso, se conduzca al usuario a tal reclamo de marketing, salvo que expresamente lo haya autorizado, por cuanto para ello, además, se ha de nutrir necesariamente de información personal.

Siguiendo con el análisis de las obligaciones, en el mismo art. 6, apartado 9 se recoge otro exhorto a los guardianes de acceso para que permitan, tanto al usuario final cuanto a terceros autorizados por éste, solicitar de manera gratuita la portabilidad de su información, ya sean los datos aportados como los generados por su uso del servicio básico de plataforma. Esta exigencia se deriva del derecho a la portabilidad de los datos, reconocido *ex novo* por el RGPD, ex artículo 20, pasando a integrar la lista ampliada de los anteriormente conocidos como derechos ARCO. Por tanto, esta obligación no supone ninguna novedad real sino, más bien, una reiteración y reafirmación de la vinculación de los “gatekeepers” con el cumplimiento de tal mandato.

Por otro lado, el apartado 10 del mismo art. 6, – adoleciendo de una redacción ciertamente farragosa, con remembranzas al famoso diálogo de los “hermanos Marx”¹⁶ –, obliga a las plataformas, si así lo solicitan, a facilitar a los usuarios profesionales y a terceros autorizados por estos, de manera gratuita, el acceso efectivo y la utilización en tiempo real de los datos personales (agregados o desagregados) generados en el uso del servicio básico de plataforma, ya sea por dichos usuarios profesionales o por sus clientes. Cabe añadir, no obstante, que la norma limita dicha posibilidad a los casos en que, primero, la información esté directamente relacionada “con el uso que los usuarios finales hayan hecho con respecto a los productos o servicios ofrecidos por el usuario profesional de que se trate a través del servicio básico de plataforma” y, segundo, medie el consentimiento expreso del usuario final para tal intercambio. Llegados a este punto, es preciso mencionar que el Supervisor Europeo de Protección de datos ya mostró su disconformidad con tal previsión¹⁷, desde su inclusión en fase de propuesta de la norma. Así, en su Opinión 2/2021 sobre la propuesta de Reglamento de Mercados digitales,

16. Artículo 6.10 “El guardián de acceso proporcionará a los usuarios profesionales y a terceros autorizados por un usuario profesional, a petición de estos y de forma gratuita, el acceso efectivo, de calidad, continuo y en tiempo real a los datos agregados o desagregados, y el uso de tales datos, incluidos los datos personales, que se proporcionen o se generen en el contexto de la utilización de los servicios básicos de plataforma o de los servicios prestados junto con los servicios básicos de plataforma pertinentes, o en apoyo de tales servicios, por parte de dichos usuarios profesionales y de los usuarios finales que recurran a los productos o servicios prestados por dichos usuarios profesionales. [...]”.

17. Para un análisis más detallado de esta cuestión, *vid.* RECIO GAYO, M., “European Union Digital Strategy: overlaps and gaps on data protection? A critical view for a better digital society and economy”, *Derecho Digital e Innovación*, núm.10, Sección Doctrina, 2021, Wolters Kluwer.

de 10 de febrero de 2021¹⁸, sostenía que ésta, en su literalidad, “podía generar confusión que conduciría a una posible incompatibilidad con el RGPD, dado que la información agregada y no agregada puede incluir en la práctica datos personales”, poniendo el énfasis en que “los datos de consulta, clics y los relativos a las búsquedas generadas por las personas constituyen datos personales”¹⁹.

Continuando con el análisis de las obligaciones, el apartado siguiente, número 11, del precitado art. 6, determina que los guardianes de acceso deberán facilitar a los prestadores de servicios de motores de búsqueda online el acceso, “en condiciones equitativas, razonables y no discriminatorias”, a datos sobre clasificaciones, consultas, clics y visualizaciones generados por los usuarios finales al hacer uso de tales servicios, tanto en las búsquedas gratuitas, como en las de pago. En todo caso, dicho mandato se amplía en los supuestos en que dicha información constituya un dato de carácter personal o lo contenga, en los que, antes de facilitarlos deberá someterlos al debido proceso de *anonimización*.

La plataforma, ex art. 8, tendrá que garantizar el efectivo cumplimiento de estas obligaciones, mediante la aplicación de las medidas pertinentes conducentes a tal fin. En este sentido, el art. 8.2 reconoce a la Comisión la potestad de incoar un procedimiento de inspección, que también podrá solicitar la propia plataforma, con el ánimo de verificar la observancia de los mandatos contenidos en los artículos precedentes, pudiendo adoptar un auto de ejecución especificando medidas que deberá adoptar el guardián de acceso.

3. OTRAS OBLIGACIONES RELACIONADAS: AUDITORÍA Y COMPROBACIÓN Y RESPONSABILIDAD

El seguimiento de todas las obligaciones recogidas en la norma queda garantizado por la imposición de otros mandatos impuestos a los guardianes de acceso que, paralelamente, se configuran como potestades de fiscalización de la Comisión.

Así, en primer lugar, el artículo 15 establece unas obligaciones de auditoría impuestas a los “gatekeepers”, los cuales, en un plazo de seis meses a contar desde su designación como tales, habrán de remitir a la Comisión una “descripción auditada independientemente” de aquellas técnicas que empleen para el perfilado de los usuarios de su servicio básico, que será redirigida al Comité Europeo de Protección de datos. Vinculado a ello, el art. 21 reconoce a la Comisión la prerrogativa de realizar solicitudes de información, por la vía de una mera reclamación o valiéndose de una decisión, exigiendo a la plataforma en cuestión

18. Fuente: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf.

19. Traducción de la autora. Texto original en inglés: “may cause confusion that could lead to inconsistency with the GDPR”, (...) “aggregated or non-aggregated data might include personal data”, (...) “query, click and view data in relation to searches generated by individuals constitute personal data”.

toda la información que acredite el cumplimiento de las obligaciones contempladas en la norma, al igual que para reclamar el acceso a cualquier tipo de dato o algoritmo que empleen y la información sobre las pruebas que efectúen con estos últimos. Para facilitar esta labor, la norma reconoce a la Comisión facultades para realizar entrevistas (art. 22) e inspecciones (art. 23), pudiendo adoptar, en su caso, medidas cautelares (art. 24). Por otro lado, en el marco de dicho procedimiento, el guardián puede adoptar compromisos para los correspondientes servicios básicos de plataforma que garanticen el cumplimiento de las obligaciones establecidas en los artículos 5, 6 y 7.

Con el mismo objetivo de permitir la comprobación de la observación por la plataforma de los mandatos analizados, desde el punto de vista interno de la organización, el Reglamento (artículo 25) determina la obligatoriedad de que cada guardián de acceso constituya en su seno un "órgano de comprobación del cumplimiento", que deberá estar integrado por uno o varios agentes con la debida cualificación (agentes de cumplimiento) y un responsable de comprobación de cumplimiento, quien habrá de ser necesariamente un alto directivo independiente. Si se constata un incumplimiento, la Comisión adoptará un auto de ejecución.

Por último, es importante reseñar las consecuencias que, de acuerdo con la norma, habrán de afrontar aquellas plataformas infractoras. Así, la LMD establece un régimen sancionador en los artículos 30 y 31. En él se contempla que la Comisión podrá imponer multas que supongan hasta el 10% del volumen de negocios total anual mundial de la empresa, o el 20% en caso de infracciones reiteradas, y multas coercitivas periódicas de hasta el 5% del volumen de negocios total diario mundial de la empresa; previendo, además, para el caso de infracciones sistemáticas, la viabilidad de aplicar medidas correctoras adicionales.

III. APUNTES FINALES

El mercado digital actual aún a un amplio listado de servicios muy diversos entre sí, conformado por un conglomerado de prestadores, de mayor o menor tamaño. Sin embargo, se ha evidenciado que un pequeño grupo de ellas ha acumulado un gran poder, aglutinando a un elevadísimo número de usuarios, lo que las sitúa en una posición hegemónica y aventajada. Ello ha supuesto la aparición de determinadas barreras de entrada, que limitan la competitividad.

Consciente de ello, el legislador europeo ha desarrollado un paquete normativo para la regulación del mercado de servicios, compuesto por dos importantes normas: el Reglamento de Servicios Digitales y el Reglamento de Mercados Digitales (LMD), que ha constituido el objeto nuclear de este estudio.

La LMD centra su regulación en un ámbito subjetivo muy específico: el de las grandes empresas, o grupos empresariales, que, prestando alguno/s del/de los servicios básicos de plataforma y cumpliendo determinados requisitos determinados

por la norma, son definidas como “guardianes de acceso” y se les impone una serie de obligaciones de diversa índole. De entre ellas, hemos resaltado por su indudable interés las relacionadas con la tutela de los datos de carácter personal, una de las principales ventajas que contribuyen a la hegemonía de esos grandes prestadores, por el amplio volumen de datos a los que acceden para su tratamiento. Especial atención hemos prestado a las obligaciones de transparencia.

Pues bien, sin perjuicio de la valoración positiva que merece el avance que supone la atención del legislador europeo a estas herramientas potencialmente lesivas de un derecho fundamental, a nuestro juicio, la regulación contenida en la norma adolece de cierta tibieza en algunos aspectos. Así, por ejemplo, hemos tenido ocasión de señalar que, de un lado, se podrían haber aplicado de manera extensiva los principios de “privacidad desde el diseño” y “por defecto”, ya creados por la normativa específica de protección de datos, que habrían contribuido a una mejor tutela de la información personal en este contexto. Asimismo, como hemos apuntado, se han obviado ciertas reticencias ya manifestadas por el Supervisor Europeo de Protección de datos en relación con algunas de las previsiones recogidas en la norma.

Por otro lado, albergamos ciertas dudas acerca de la efectividad práctica de la exigencia a las plataformas, prevista la LMD, de que garanticen que los usuarios finales tengan la posibilidad de escoger no autorizar el tratamiento de su información, obteniendo un servicio de la misma calidad. Eso, como bien reconoce el propio texto normativo, no es viable, por cuanto al no poder perfilar al usuario, la plataforma siempre se podrá escudar en la imposibilidad de mantener los mismos estándares y así acogerse a la excepción que contempla la norma para eximir las de su cumplimiento.

Asimismo, mostramos una postura crítica en relación a la opción abierta, que reconoce el Reglamento a la Comisión, para designar como guardián de acceso a plataformas que no cumplan todos los requisitos exigidos por el propio texto legal; y ello porque consideramos que contribuye a crear una indeseable inseguridad jurídica en el mercado. Idéntica opinión nos merece la decisión del legislador europeo de reenviar o remitir a otras normas la definición de determinados conceptos clave, especialmente los que relativos a las tipologías de servicio básico de plataforma contempladas en el Reglamento.

En cuanto a los objetivos básicos de esta nueva iniciativa legislativa europea está el fomento de la libre competencia en el mercado digital de servicios, por lo que viene a complementar la normativa preexistente sobre la materia, haciendo especial hincapié en las obligaciones de transparencia y rendición de cuentas de las grandes plataformas prestadoras de servicios básicos. En tal sentido, como afirma MONTERO GARCÍA-NOBLEJAS, *“La Ley de Mercados Digitales avanza un paso más, en la medida en que se trata de un sistema que permite una aplicación ex ante, tiene carácter horizontal y no va a depender de estudios de mercado*

previos desarrollados caso por caso, como sucede con el derecho de la competencia tradicional”²⁰.

A la luz de todo lo anterior, no podemos más que aplaudir la contribución a tal fin que supone este nuevo paquete de medidas europeo, si bien con las “luces y sombras” que hemos ido desgranando en este estudio.

IV. BIBLIOGRAFÍA

ÁLVAREZ MORENO, La contratación electrónica mediante plataformas en línea: modelo negocial (B2C), Editorial Reus, 2021.

MADRID PARRA, A., “Aproximación inicial a los Reglamentos Europeos sobre servicios y mercados digitales”, *La Ley Unión Europea*, núm. 110, enero 2023.

MONTERO GARCÍA-NOBLEJAS, M. P., “El reto regulatorio de una economía basada en plataformas digitales”, *LA LEY mercantil*, núm. 99, Sección Derecho digital/ Doctrina, 2023.

MORALES BARCELÓ, J., “Los guardianes de acceso y la dudosa necesidad de la propuesta de ley de mercados digitales: especial referencia a las concentraciones económicas”, *Revista de Derecho de la Competencia y la Distribución*, núm. 28, Sección Estudios, 2021, Wolters Kluwer.

OROZCO GONZÁLEZ, M., “La utilización ilícita de datos de carácter personal por los partidos políticos”, *Actualidad civil*, núm. 7, 2021.

RECIO GAYO, M., “European Union Digital Strategy: overlaps and gaps on data protection? A critical view for a better digital society and economy”, *Derecho Digital e Innovación*, núm.10, Sección Doctrina, 2021, Wolters Kluwer.

VILALTA NICUESA, A. E., “La regulación europea de las plataformas digitales en la era de la economía colaborativa”, *RCDI*, núm. 765, 2018.

Comisión Europea, de 31 de octubre de 2022, QANDA/20/2349, “Preguntas y respuestas: Ley de Mercados Digitales: garantizar unos mercados digitales justos y abiertos”.

Supervisor Europeo de Protección de Datos, Opinión 2/2021 sobre la propuesta de Reglamento de Mercados digitales, de 10 de febrero de 2021.

UNCTAD “Technical Notes on ICT for Development. ESTIMATES OF GLOBAL E-COMMERCE 2019 AND PRELIMINARY ASSESSMENT OF COVID-19 IMPACT ON ONLINE RETAIL 2020”, publicado en 2021.

20. MONTERO GARCÍA-NOBLEJAS, M. P., “El reto regulatorio de una economía basada en plataformas digitales”, *LA LEY mercantil*, núm. 99, Sección Derecho digital / Doctrina, 2023; p. 23.

