Prácticas comerciales personalizadas mediante sistemas de IA

La explotación desleal de datos sensibles y factores de vulnerabilidad

Irene Sánchez Frías

Marcial Pons

PRÁCTICAS COMERCIALES PERSONALIZADAS MEDIANTE SISTEMAS DE INTELIGENCIA ARTIFICIAL

La explotación desleal de datos sensibles y factores de vulnerabilidad

IRENE SÁNCHEZ FRÍAS

PRÁCTICAS COMERCIALES PERSONALIZADAS MEDIANTE SISTEMAS DE INTELIGENCIA ARTIFICIAL

La explotación desleal de datos sensibles y factores de vulnerabilidad

Prólogo de
Eugenio Olmedo Peralta

Marcial Pons
MADRID | BARCELONA | BUENOS AIRES | SÃO PAULO
2026

Esta obra ha sido realizada y publicada en el marco de las actividades del proyecto CODIG-IA (marco jurídico para la competencia dinámica en mercados digitales y para la innovación a través de inteligencia artificial, PID2021-122536OB-I00), del que es IP el profesor Eugenio Olmedo Peralta, así como del proyecto CoMeDi (consumidores y pequeños profesionales en la contratación en Mercados Digitales: prácticas anticompetitivas, desleales y explotación de dependencia económica, Ref. ProyExcel_00665, PAIDI 2020), del que son IPs los profesores Eugenio Olmedo Peralta y Patricia Benavides Velasco.



Irene Sánchez Frías es profesora colaboradora doctora en la Universidad Cardenal Herrera-CEU, CEU Universities.



Quedan rigurosamente prohibidas, sin la autorización escrita de los titulares del *copyright*, bajo las sanciones establecidas en las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares de ella mediante alquiler o préstamo públicos.

© Irene Sánchez Frías
© MARCIAL PONS
EDICIONES JURÍDICAS Y SOCIALES, S.A.
Tamayo y Baus, 7, 1.º izq. 28004 MADRID
☎ 91 304 33 03
www.marcialpons.es

ISBN: 979-13-87913-49-6
Depósito legal: M 28191-2025
DOI: *10.37417/practicas-comerciales-personalizadas-mediante-sistemas-ia*

Diseño de cubierta: ene estudio gráfico

Impresión: Élece, Industrias Gráficas, S.L.

MADRID, 2026

A mi abuela Mari,
tack så mycket

ÍNDICE

Pág.

NOTA AL LECTOR 19

AGRADECIMIENTOS 21

PRÓLOGO, *por Eugenio Olmedo Peralta* 23

ABREVIATURAS 33

INTRODUCCIÓN 35

PRIMERA PARTE

LA PROHIBICIÓN DE PRESENTAR ANUNCIOS BASADOS EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES EN LAS PLATAFORMAS EN LÍNEA. IDENTIFICACIÓN DE LAS PRINCIPALES PROBLEMÁTICAS E INTERACCIONES ENTRE LA DSA, LA DMA Y EL RGPD

CAPÍTULO I. **ÁMBITO OBJETIVO DE LA PROHIBICIÓN. PRESENTAR ANUNCIOS BASADOS EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES** 43

I. NOTAS PREVIAS SOBRE EL FUNCIONAMIENTO DE LA PUBLICIDAD *ONLINE* PERSONALIZADA 43

1. Categorías de publicidad *online* personalizada 43
2. Formatos en los que puede presentarse la publicidad *online* personalizada y su remuneración 45

Pág.

II. ACTORES EN LA PUBLICIDAD DIGITAL..... 48
III. CONTEXTO Y JUSTIFICACIÓN DE LA PROHIBICIÓN DE PRESENTAR ANUNCIOS BASADOS EN PERFILES QUE UTILICEN DATOS SENSIBLES 49
IV. LA ACTIVIDAD PROHIBIDA: «PRESENTAR» PUBLICIDAD BASADA EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES 51
V. LA REFORMULACIÓN DEL TÉRMINO «ANUNCIO» O «PUBLICIDAD», EN LA DSA. EXCLUSIÓN DE PRÁCTICAS PERSONALIZADAS QUE NO SEAN PUBLICIDAD 55
1. Análisis comparado del concepto de publicidad en la normativa de la UE, la normativa nacional y la DSA 55
2. Interacciones con el Reglamento sobre transparencia y segmentación en la publicidad política 61
VI. LA PUBLICIDAD BASADA EN «LA ELABORACIÓN DE PERFILES»..... 63
1. El uso de medios automatizados para la elaboración de perfiles: algoritmos, análisis de *big data* e inteligencia artificial 64
2. Tipos de perfiles englobados en la prohibición..... 66
VII. LA UTILIZACIÓN DE «CATEGORÍAS ESPECIALES DE DATOS PERSONALES», EN LA PUBLICIDAD BASADA EN PERFILES. LA REMISIÓN AL RGPD Y SU PRIMACÍA COMO NORMA DE CONFLICTO..... 70

CAPÍTULO II. **LA NOCIÓN DE DATOS SENSIBLES Y SU CONCEPTUALIZACIÓN EN EL RGPD. NATURALEZA DE LOS DATOS INFERIDOS Y LOS *PROXIES*, Y DATOS NO INCLUIDOS EN LA LISTA DE DATOS SENSIBLES**..... 73

I. EL CONCEPTO DE DATOS PERSONALES Y SU TRATAMIENTO 73
II. ¿SON LOS DATOS INFERIDOS DATOS PERSONALES? 78
III. CONCEPTO, RAZÓN DE SER Y TIPOLOGÍA DE DATOS PERSONALES SENSIBLES. EL PROBLEMA DE LOS PROXIES Y LOS DATOS SENSIBLES INFERIDOS 84
1. Concepto, antecedentes y razón de ser de los datos sensibles 84
2. La disyuntiva de la naturaleza de los *proxies* y los datos inferidos..... 88

Pág.

2.1. Datos genéticos 92
2.2. Datos biométricos 95
2.3. Datos relativos a la salud 103
2.4. Datos reveladores del origen étnico o racial 108
2.5. Datos reveladores de opiniones políticas 112
2.6. Datos reveladores de afiliación sindical 114
2.7. Datos relativos a convicciones religiosas o filosóficas 117
2.8. Datos relativos a la vida sexual u orientación sexual 120

IV. ¿DEVALUACIÓN DEL CONCEPTO «DATOS PERSONALES SENSIBLES» BAJO UNA INTERPRETACIÓN FUNCIONAL? LA SENSIBILIDAD POR DISTANCIA COMO CONTRAPESO 122
V. DATOS PERSONALES NO INCLUIDOS EN LA LISTA DE DATOS SENSIBLES DEL RGPD 127

CAPÍTULO III. **ÁMBITO SUBJETIVO DE LA PROHIBICIÓN: LOS PRESTADORES DE PLATAFORMAS EN LÍNEA** 135

I. ACLARACIONES TERMINOLÓGICAS PREVIAS EN TORNO AL CONCEPTO DE PLATAFORMA. DIFERENCIAS RELEVANTES ENTRE LA NOCIÓN DE PLATAFORMAS EN LÍNEA DE LA DSA Y LA DE SERVICIOS BÁSICOS DE PLATAFORMA DE LA DMA 135
1. Diferente ámbito material de ambas categorías: servicios intermediarios (DSA) y servicios de intermediación (DMA) 136
2. La designación del prestador del servicio de plataforma 138
3. El servicio caracterizador 143

II. LA REFORMULACIÓN DEL TÉRMINO «DIFUSIÓN AL PÚBLICO», EN LA DSA. ¿EXCLUSIÓN DE CIERTOS SERVICIOS? 148
III. LA DELIMITACIÓN DE LOS SERVICIOS INTEGRADOS BAJO LA PERSPECTIVA DE LA DSA 152
1. Perspectivas unitarias. Tendencias a considerar el servicio de publicidad y el servicio principal como un servicio «indisoluble» 152
2. Perspectivas delimitadoras. Indicadores a favor de delimi-

Pág.

tar el servicio principal y el servicio de publicidad 155
2.1. La DMA y la regulación de los «servicios integrados» 155
2.2. La delimitación de los servicios integrados bajo la DSA 158

IV. ¿ES SIEMPRE UN SERVICIO INTERMEDIARIO DE PUBLICIDAD EN LÍNEA UN SERVICIO DE PLATAFORMA? POSIBLES EXCEPCIONES BAJO LA DSA 163
V. ¿DEBERÍAN LOS GRANDES SERVICIOS DE INTERMEDIACIÓN PUBLICITARIA (ALPHABET ADVERTISING, META ADS Y AMAZON ADS) SER DESIGNADOS COMO VLOPS? 167
VI. MEDIDAS DE COMPLIANCE A EJECUTAR POR CADA PRESTADOR IMPLICADO EN SERVICIOS QUE INTEGREN PUBLICIDAD *ONLINE* BASADA EN PERFILES. 172
VII. MEDIDAS ADICIONALES DE TRANSPARENCIA PUBLICITARIA APLICABLES A LAS VLOP 179

SEGUNDA PARTE
LA EXPLOTACIÓN DE DATOS PERSONALES Y VULNERABILIDADES EN LAS PRÁCTICAS COMERCIALES BASADAS EN PERFILES. UN ANÁLISIS DESDE LA COMPETENCIA DESLEAL

CAPÍTULO IV. **INFRACCIONES EN EL TRATAMIENTO, LA COMBINACIÓN Y LA EXPLOTACIÓN ILÍCITOS DE DATOS PERSONALES PARA LA OFERTA DE PUBLICIDAD BASADA EN PERFILES. UN REPROCHE DE DESLEALTAD POR VIOLACIÓN DE NORMAS** 183

I. CONTEXTO ACTUAL DE LA VIOLACIÓN DE NORMAS 183
II. NOTAS PREVIAS EN TORNO A LA VIOLACIÓN DE NORMAS COMO PRÁCTICA DESLEAL 186
1. Cuestiones generales y finalidad del precepto 186
2. Normas cuya vulneración puede activar la aplicación del precepto 188
3. La distinción entre normas concurrenciales y no concurrenciales 189

Pág.

III. VIOLACIÓN DE NORMAS POR ILICITUD DE LA BASE LEGAL APLICADA AL TRATAMIENTO DE DATOS PERSONALES CON FINES DE PUBLICIDAD PERSONALIZADA. INFRACCIONES DEL RGPD 191

1. Identificación de la norma vulnerada. ¿Es el RGPD una norma amparada por el art. 15 LCD? 191
2. Calificación de la norma: El RGPD como norma no concurrencial 193
3. Examen legal bajo el art. 15.1 LCD 195

3.1. La infracción normativa. Ilicitud de la base legal aplicada para el tratamiento de datos personales conforme al RGPD 195

3.2. Adquisición de una ventaja competitiva significativa como resultado del tratamiento ilícito de datos personales 200

IV. VIOLACIÓN DE NORMAS POR COMBINACIÓN ILÍCITA DE DATOS PERSONALES CON FINES DE PUBLICIDAD PERSONALIZADA. INFRACCIÓN CUMULATIVA DE LA DMA Y DEL RGPD 206

1. La combinación de datos personales con fines publicitarios 206
2. Identificación de la norma vulnerada: el art. 5.2 de la DMA 209
3. Calificación de la norma: la DMA como norma concurrencial 211
4. Consecuencias de tratar al art. 5.2 DMA como una norma concurrencial. La presunción del art. 15.2 LCD 214

V. VIOLACIÓN DE NORMAS POR EXPLOTACIÓN ILÍCITA CONFORME A LA DSA. LA PRESENTACIÓN DE PUBLICIDAD BASADA EN PERFILES UTILIZANDO DATOS SENSIBLES 215

1. Identificación de la norma vulnerada. ¿Se somete la infracción del art. 26.3 de la DSA al ámbito de aplicación general del art. 15 LCD? 215
2. Calificación de la norma. La DSA como norma no concurrencial 216
3. Examen legal bajo el art. 15.1 LCD 217

Pág.

VI. REFLEXIONES FINALES. PROBLEMAS APLICATIVOS DEL ILÍCITO DE DESLEALTAD DE LA VIOLACIÓN DE NORMAS AL USO DE DATOS SENSIBLES EN LA ACTIVIDAD PUBLICITARIA 219

CAPÍTULO V. **LAS PRÁCTICAS COMERCIALES BASADAS EN PERFILES QUE EXPLOTEN VULNERABILIDADES DEL DESTINATARIO. REPROCHE DE DESLEALTAD BAJO LA MODALIDAD DE PRÁCTICAS AGRESIVAS Y BAJO LA CLÁUSULA GENERAL** 223

I. LA RELACIÓN DE COMPLEMENTARIEDAD ENTRE LA DPCD, EL RGPD Y LA DSA 223
II. EL ÁMBITO DE APLICACIÓN DE LA DPCD Y LA LCD 228
1. El ámbito de aplicación personal. Divergencias entre la DPCD y la LCD..... 228
2. El ámbito de aplicación material. La publicidad basada en perfiles bajo los conceptos de acto de competencia desleal (LCD) y práctica comercial (DPCD) 231
2.1. Consideraciones generales 231
2.2. Especial referencia a la exclusión de determinados destinatarios 236
2.3. La publicidad basada en perfiles que no guarde relación (directa ni indirecta) con la contratación de productos y servicios..... 237
III. BREVE REFERENCIA AL EXAMEN DE TRES PASOS Y A LA LISTA NEGRA DE PRÁCTICAS DESLEALES HACIA LOS CONSUMIDORES 238
IV. EXAMEN DE DESLEALTAD DE LAS PRÁCTICAS COMERCIALES QUE EXPLOTEN DATOS PERSONALES REVELADORES DE VULNERABILIDAD..... 240
1. Encuadre y caracterización como práctica agresiva..... 240
2. Medios de agresividad. La relevancia del contexto y las líneas grises entre el acoso y la influencia indebida: ¿es necesaria una diferenciación? 242
3. La afectación del comportamiento económico..... 248
3.1. La merma significativa de la libertad de elección con relación al bien o servicio..... 249

Pág.

3.2. La toma (o posible toma) de una decisión sobre una transacción que de otro modo no hubiera adoptado 255
4. El consumidor medio como referencia para el examen de deslealtad 257
V. EXAMEN BAJO LA CLÁUSULA GENERAL DE DESLEALTAD 263
1. Cuestiones generales sobre la cláusula general 263
2. El incumplimiento de la diligencia profesional 266
3. La aptitud para distorsionar de forma significativa el comportamiento económico del consumidor 272
4. Prácticas comerciales dirigidas a grupos concretos de consumidores: el parámetro del miembro medio del grupo ... 273
5. Prácticas comerciales que afecten únicamente a grupos identificables de consumidores vulnerables 276
VI. NOTAS FINALES 280

TERCERA PARTE
PRÁCTICAS COMERCIALES PERSONALIZADAS QUE EXPLOTEN VULNERABILIDADES MEDIANTE SISTEMAS DE IA

CAPÍTULO VI. **PRÁCTICAS COMERCIALES MANIPULADORAS, SUBLIMINALES O EXPLOTADORAS DE VULNERABILIDADES MEDIANTE SISTEMAS DE IA** .. 285

I. ALGUNAS NOCIONES PREVIAS SOBRE LAS PRÁCTICAS COMERCIALES PERSONALIZADAS MEDIANTE SISTEMAS DE IA 285
1. Justificación del examen: carencias de la prohibición de la DSA y relaciones entre la DPCD y la AIA 285
2. La noción de sistemas de IA en la AIA 288
2.1. El sistema debe estar basado en una máquina 289
2.2. El sistema debe estar diseñado para funcionar con distintos niveles de autonomía 291
2.3. La posible capacidad de adaptación tras el despliegue 293

Pág.

2.4. La capacidad de realizar inferencias para generar outputs 293
2.5. La posible capacidad de influencia en entornos físicos o virtuales 297

II. PRÁCTICAS COMERCIALES PERSONALIZADAS MANIPULATIVAS O SUBLIMINALES DESARROLLADAS A PARTIR DE SISTEMAS DE IA. UN EXAMEN BAJO EL CATÁLOGO DE PROHIBICIONES DE LA AIA 298

1. La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA. Sujetos obligados por las prohibiciones del art. 5 AIA 299
2. La utilización de técnicas subliminales que transciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas 301

2.1. La utilización de técnicas subliminales que transciendan la conciencia de una persona (física) 302
2.2. La utilización de técnicas deliberadamente manipulativas o engañosas 307

3. Su objetivo o efecto: la alteración sustancial del comportamiento de una persona o un colectivo de personas 313

3.1. La alternatividad entre «objetivo» o «efecto», en la alteración comportamental 313
3.2. La alteración sustancial del comportamiento 315

4. La merma apreciable de la capacidad de tomar una decisión informada 317
5. La toma de una decisión que, de otro modo, no se hubiese tomado 319
6. La provocación o probabilidad de provocación de perjuicios considerables 320

6.1. La provocación o probabilidad de provocación de un perjuicio 321
6.2. La magnitud «considerable» del perjuicio y tipos de perjuicios englobados 322
6.3. El sujeto perjudicado por la práctica manipulativa o subliminal: la persona afectada, otra persona o un colectivo 326

III. PRÁCTICAS COMERCIALES EXPLOTADORAS DE VULNERABILIDADES 329

Pág.

1. El concepto de vulnerabilidad 329
2. Similitudes y diferencias reseñables con respecto a las prácticas de IA manipulativas o subliminales 331
3. La explotación de vulnerabilidades a través de sistemas de IA 333
4. Concreción de los sujetos pasivos: causas de vulnerabilidad del art. 5.1.*b)* AIA y prácticas prohibidas combinadas 335

IV. CONSECUENCIAS DERIVADAS DE LA INFRACCIÓN DE LAS PROHIBICIONES DE LA AIA Y SU CONVIVENCIA CON OTRAS INFRACCIONES PARALELAS BAJO LOS PRINCIPIOS DE PROPORCIONALIDAD Y *NE BIS IN IDEM* 339

V. VALORACIONES FINALES 340

CONCLUSIONES 343

I. LA ASEPSIA DE LAS PROHIBICIONES ABSOLUTAS ANTE LOS EFECTOS POSITIVOS DE LOS PERFILES PUBLICITARIOS QUE UTILIZAN DATOS SENSIBLES 344

II. REMISIONES AL RGPD, LA OBSOLESCENCIA DEL CONCEPTO DE DATOS SENSIBLES Y SU HERENCIA (SIN BENEFICIO DE INVENTARIO) 346

III. LA NOCIÓN DE PLATAFORMA Y LA INCIERTA REFORMULACIÓN DEL CONCEPTO DE DIFUSIÓN AL PÚBLICO 347

IV. LA LISTA DE VLOPS Y LA NO INCLUSIÓN DE LOS SERVICIOS DE INTERMEDIACIÓN PUBLICITARIA 348

V. LA VIOLACIÓN DE NORMAS POR INFRACCIÓN DEL RGPD Y LAS DIFICULTADES PARA SU APLICACIÓN POR EL JUEZ NACIONAL 349

VI. LÍMITES A LAS FLEXIBILIZACIONES INTERPRETATIVAS DE LA DPCD 350

VII. LA AIA Y LA DPCD: UN MATRIMONIO BIEN AVENIDO 351

VIII. QUÉ ES SER VULNERABLES, SI TODOS SOMOS VULNERABLES 352

IX. LA HIPERREGULACIÓN DE LAS PRÁCTICAS COMERCIALES PERSONALIZADAS 352

BIBLIOGRAFÍA 355

NOTA AL LECTOR

La presente obra fue finalizada y entregada para su publicación en septiembre de 2025. En consecuencia, todas las referencias temporales contenidas en ella —en particular, las expresiones «hasta la fecha», «en la actualidad» u otras equivalentes— deben entenderse referidas a dicho momento.

Las resoluciones y novedades posteriores serán analizadas por la autora en una publicación posterior. Entre ellas se encuentra, en particular, la sentencia dictada en el asunto *AMI contra Meta* por el Juzgado de lo Mercantil núm. 15 de Madrid (ECLI:ES:JM:2025:128).

AGRADECIMIENTOS

Esta obra tiene su origen en la tesis doctoral que desarrollé en la Universidad de Málaga bajo la dirección del profesor Eugenio Olmedo Peralta y que fue defendida ante un tribunal integrado por los profesores Pablo Fernández Carballo-Calero, Jaume Martí Miravalls y Mariateresa Maggiolino. La obra, al igual que su autora, no es más que el fruto de una inversión colectiva.

A esta inversión colectiva corresponden una serie de reconocimientos transfronterizos que explican cualquier valor que pueda tener la obra.

Comenzando por Málaga, mi hogar, el primer agradecimiento debe ser a mi familia. En especial a mis padres y a mi hermano Alejandro. Gracias por ser fortaleza en mi vulnerabilidad.

Sigo con quien es, y siempre será, mi padre académico: el profesor Eugenio Olmedo Peralta. A Eugenio podría agradecerle muchas cosas, la menor de todas (en absoluto menor) serían las correcciones a esta obra. A ella van unidas sus múltiples respuestas a mis no pocas preguntas, que nunca recibe como tontas. El carácter de Eugenio, su buena disposición, su sentido del humor y, sobre todo, su entusiasmo han dado vida a mis inicios como investigadora. Eugenio «me regaña» cuando escribo párrafos largos; aun así, siento que a este agradecimiento siempre le faltarán líneas. Abrevio diciendo que lo que más le agradeceré, siempre, es que me valora como soy… sin dejar de creer en todo lo que puedo ser.

No puedo dejar de mencionar a mis amigas de toda la vida. Patri, Paqui Belén, Andrea y Elena. Gracias por ser el repositorio de mis da-

tos sensibles (que, en conjunto, son todos). También a Rafa, por haber crecido a mi lado, y a su familia.

Tampoco puedo dejar de citar a mi Escuela, que no es otra que el Área de Derecho Mercantil de la Universidad de Málaga. Me debo a cada uno de los profesores que la conforman. Todos me han enseñado algo bueno.

Continúo con Bruselas, si bien no pudo haber Bruselas sin previamente Málaga. De Málaga y de Ronda era el maestro don Manuel Olivencia, a cuyo justo homenaje debo mi Máster en Propiedad Intelectual y Derecho de las TIC en KU Leuven. Gracias a la Fundación Cuatrecasas por apostar a favor de una chica con más inquietudes que respuestas. A esta generosa oportunidad debo todos los años sucesivos.

Bruselas no puede contemplarse sin todos los amigos que hice allí. Casi veinte personas, cada una con su origen (Grecia, Italia, Bélgica, Polonia…) me hicieron creer en el sentido del lema *in varietate concordia*. Gracias especialmente a Elena, Konstantinos, Elli, Alessandro, Sara, María y Andrea. Siempre que pienso en vosotros sonrío.

Sigo con el siguiente destino, Glasgow. Gracias a todos los profesores de la Facultad de Derecho de la Universidad de Strathclyde, por acoger con cariño a una joven angustiada, como cualquier doctorando, con el final de su tesis. Especialmente al profesor Barry Rodger, a quien debo agradecer el acceso a una Facultad llena de personas estupendas, así como otros regalos (entrenarme en el acento escocés, sus recomendaciones de turismo por las Highlands, el *haggis*…). Pero lo que más le agradezco es que me dedicara, generosamente y *motu proprio*, su tiempo, que es lo que menos tenía. Gracias también al profesor Linus Hoffmann, por estar siempre dispuesto a escucharme y entenderme, y por transmitirme su entusiasmo por la investigación.

Cierro con Bolonia, mi actual destino. Gracias al Colegio de España en Bolonia, a don Gil Álvarez de Albornoz y a su Rector, el profesor Juan Gutiérrez Alonso.

Como no podía ser de otra manera, gracias a todos los Colegiales. La grandeza (y al mismo tiempo sencillez) que hay en cada uno de vosotros me ha hecho crecer y querer seguir creciendo. Me perdonarán la licencia de reconocer en especial a Aido, Gortázar y Salazar, por mirarme con los ojos del cariño, por cuidarme, por mantenerme *ancora viva* y feliz. Dais honor y sentido al Colegio.

A Julio, por su generosidad al proponer compartir su vida conmigo.

Gracias a todos.

PRÓLOGO

I. DE LO VISIBLE Y LO INVISIBLE, LO JUSTO Y LO INJUSTO

Una de las más bellas reflexiones sobre la justicia, la naturaleza humana y la moral la encontramos en *La República* de Platón, con ocasión de la metáfora del anillo de Giges. Glaucón narra que Giges era un pastor lidio que tras un terremoto se coló por una brecha abierta en la tierra, encontrando una cueva en la que descubrió un caballo de bronce que, a modo de sepultura, albergaba un cadáver desnudo que portaba un anillo de oro en un dedo. Tras salir de allí con el tesoro en su poder, Giges descubrió que el anillo era prodigioso: llevándolo puesto, al volver la piedra preciosa de la sortija hacia el lado interior de la mano, conseguía hacerse invisible. Volviendo a poner la piedra por el lado de afuera, se revertía el efecto y su portador volvía a su estado natural. Aprovechando el nuevo poder que había adquirido, Giges se dirigió al palacio del rey de Lidia, sedujo a la reina y, con ayuda del anillo, se deshizo del rey y se apoderó del trono.

Esta metáfora permite al filósofo reflexionar sobre el comportamiento moral de las personas, justas e injustas: «si hubiera dos sortijas como aquella de las cuales llevase una puesta el justo y otra el injusto, es opinión común que no habría persona de convicciones tan firmes como para perseverar en la justicia y abstenerse en absoluto de tocar lo de los demás, cuando nada le impedía dirigirse al mercado y tomar de allí sin miedo alguno cuanto quisiera […]». Ese punto permite a Glaucón, Adimanto y Sócrates entrar a discutir sobre si fuera preferible parecer ser justo, siendo injusto, que realmente ser justo y parecer

injusto. *No hay mayor perfección en el mal que el parecer ser bueno no siéndolo*.

El pesimista dirá que la creatividad humana es limitada, incluso la de los grandes genios. Tal vez merece la pena recordar las buenas historias una y otra vez. Sobre todo, cuando nos sirven para pensar la justicia. La propia historia de Giges se inspira en el yelmo de Hades, que Hesíodo[1] narra que fue forjado por los cíclopes junto al rayo de Zeus y al tridente de Poseidón para derrocar a Cronos y los Titanes. Posteriormente, Perseo utilizaría este casco de Hades para matar a Medusa sin ser visto por las Gorgonas[2]. Este recurso a la invisibilidad como don de un objeto mágico para ayudar al héroe pasaría a la mitología germánica del siglo XIII transformándose en la capa de invisibilidad (*Tarnkappe*) de que se serviría Siegfried en la *Nibelungenlied*.

Basándose en el mito germánico, mi admirado Richard Wagner volvería a darle al objeto la forma de sortija en la magna tetralogía operística *El anillo del Nibelungo*. En este caso, el genio sajón volvió a incluir el juicio de moralidad en la forja del anillo, vinculando el uso inapropiado del mismo a la destrucción del alma de su portador. Así, al serle arrebatado el anillo, el nibelungo Alberich lo maldice:

> Su oro me otorgó un poder ilimitado, que ahora su magia traiga la muerte a aquel que lo lleve. Ningún hombre será feliz con él, ningún hombre afortunado verá la sonrisa de su resplandor. Cualquiera que lo posea se sentirá agobiado por problemas, y cualquiera que ahora lo tenga, será acosado por la envidia. Todo el mundo ansiará poseerlo, pero nadie le sacará provecho […].

«…y el señor del anillo se convertirá en su esclavo[3]». Añadiendo fantasía y alejándose de la mitología, J. R. R. Tolkien haría que el ani-

---

[1] HESÍODO, Teogonía, ed. M. L. West, Oxford, 1966, vers. 865-875:
«A éstos (a los dioses) los Cíclopes les dieron dones gloriosos:
a Zeus, el rayo, el relámpago y el trueno rugiente;
a Poseidón, el tridente, obra irresistible;
y a Hades, un casco invisible, terrible en la lucha.
Cuando con éstos dominaron a su gran padre Crono y lo encadenaron,
arrojaron entonces los dioses a los Titanes al oscuro Tártaro,
y Zeus hizo brillar la luz en el vasto éter de muchos destellos,
mostrando benignamente la tierra y el ancho cielo».

[2] APOLODORO, *Bibliotheca* II, 4, 2; PÍNDARO, *Pítica* XII, vers. 12-28:
«…y sobre sus ojos derramó la oscuridad del casco de Hades,
para que se hiciera invisible a la enemiga diosa
y evitara la mirada mortal de las hermanas Gorgonas»
(traducción de Alfonso Ortega, Píndaro, *Odas y fragmentos*, Biblioteca Clásica Gredos, núm. 68, 1984).

[3] WAGNER, R., *Rheingold*, Szene III:
«Gab sein Gold
mir Macht ohne Maß,

llo fuera la causa de perdición de Sméagol y obsesión corrompedora de Gollum. Finalmente, más cercano a los gustos de la autora de esta obra que tengo el honor de prologar, J. K. Rowling recuperaría la tradición germánica de darle al objeto forma textil para incluir la capa de invisibilidad como una de las Reliquias de la Muerte de Harry Potter, instrumento de travesuras y de heroicidades.

II. EL ESFUERZO SILENCIOSO

Este rápido recorrido por los sueños del ser humano de poder valerse de la invisibilidad para hacer su voluntad, sea esta virtuosa o deshonesta, nos lleva a la obra que presentamos. Su autora, Irene Sánchez Frías, es una joven investigadora malagueña, de raíces rondeñas (como el que suscribe), con una gran pasión por los retos actuales del derecho ante la sociedad digital. Hace unos años, cuando cursaba el Máster Universitario en Abogacía en la Universidad de Málaga, la autora se dirigió a mí para que dirigiese su tesis doctoral. La temeridad de Irene le llevó a hacerme caso en dos propuestas: la elección de un tema de investigación y la necesidad de afrontarlo desde una visión verdaderamente europea. La combinación de ambas le llevaría a desarrollar durante años la investigación que resultaría en su tesis doctoral y que, tras un concienzudo proceso de adaptación y mejora, daría lugar a la obra que el lector tiene en sus manos.

Contagiada por mi entusiasmo europeísta, Irene Sánchez ha llevado a cabo su investigación en un contexto verdaderamente internacional. En el año 2022, la autora ganó la II Beca Manuel Olivencia (¡otro mercantilista rondeño! aunque este de perfil irrepetible) de la Fundación Cuatrecasas, lo que le permitiría cursar el *Master of Intellectual Property and ICT Law* en la sede de Bruselas de la Universidad Católica de Lovaina (*KU Leuven*). En el corazón de Europa, Irene

---

nun zeug' sein Zauber
Tod dem, der ihn trägt!
Kein Froher soll
seiner sich freun,
keinem Glücklichen lache
sein lichter Glanz!
Wer ihn besitzt,
den sehre die Sorge,
und wer ihn nicht hat,
den nage der Neid!
Jeder giere
nach seinem Gut,
doch keiner genieße
mit Nutzen sein!
[…] des Ringes Herr
als des Ringes Knecht»

no solo tendría ocasión de ampliar sus conocimientos en materia de propiedad intelectual e industrial y derecho de las nuevas tecnologías, sino que, además, tendría contacto directo con el funcionamiento de las instituciones de la Unión, tan importante para comprender el sistema jurídico actual.

Tras obtener una beca de Formación de Profesorado Universitario (FPU) del Ministerio de Universidades en la Universidad de Málaga, la profesora Sánchez desarrollaría una nueva estancia de investigación en la *Strathclyde University Law School* de Glasgow, integrándose en el equipo del *Strathclyde Centre for Antitrust Law and Empirical Study*, bajo la supervisión del profesor Barry Rodger. Finalmente, en 2024 tendría la gran suerte de unirse a la *Proles Aegidiana* al obtener una Beca Santa Catalina de Bolonia para ampliar su investigación en el Real Colegio de España. Estoy convencido de que con su trabajo y esfuerzo Irene ha continuado el legado, consiguiendo que *florezcan las artes de la paz*.

Tras este paso por Bélgica, el Reino Unido e Italia —e, incluso, haber tenido tiempo para iniciarse en la actividad docente en la Universidad de Málaga— la investigación de Irene culminaría con la defensa de la tesis doctoral «Prácticas comerciales personalizadas mediante sistemas de Inteligencia Artificial. La explotación desleal de datos sensibles y factores de vulnerabilidad», defendida en la Universidad de Málaga el pasado 7 de julio de 2025 ante un tribunal presidido por el profesor Pablo Fernández Carballo-Calero (catedrático de Derecho Mercantil de la Universidad de Vigo) e integrado por los profesores Jaume Martí Miravalls (catedrático de Derecho Mercantil de la Universidad de Valencia) y Mariateresa Maggiolino (professoressa ordinaria di Diritto dell'Economia de la Università Bocconi de Milán). La tesis fue calificada con Sobresaliente Cum Laude por unanimidad, permitiendo la colación del título de Doctora Internacional.

Ducunt volentem fata, nolentem trahunt. Los hados guían a quien los sigue de buen grado y arrastran a quien se resiste[4]. En los últimos meses, la aventura académica de Irene Sánchez ha dado un nuevo giro que la ha llevado a dejar su alma mater universidad malacitana, para conducirla a mi querida tierra de Valencia, donde actualmente es profesora de Derecho mercantil en la Universidad CEU-Cardenal Herrera. Estoy convencido de que la autora sacará gran partido de la estimulante e incesante vida académica de la ciudad del Turia, confiando en que ella también pueda devolver un poquito de todo lo que aprendemos de los admirados compañeros levantinos.

---

[4] Aunque normalmente se atribuye esta máxima estoica a Séneca (*Cartas a Lucilio*, 107, 11), el cordobés la toma del filósofo Cleantes de Asos, discípulo de Zenón de Citio, primero en impartir sus lecciones desde la Stoa.

III. LA CAPA DE INVISIBILIDAD DE LAS EMPRESAS DIGITALES

Presentada la autora, corresponde ahora introducir el trabajo al que preceden estas páginas. Comenzamos este prólogo aludiendo a cómo diversos pasajes literarios se han referido al uso de distintos artefactos (anillos, capas, yelmos…) para conseguir ser invisibles y utilizar esa condición para, según la moralidad del usuario, hacer el bien o el mal. En muchos casos, las empresas que actúan en el mercado digital disfrutan también de esta cualidad de imperceptibilidad para llevar a cabo sus prácticas comerciales. Ésta es la premisa de la que parte la autora al dirigir su investigación: discernir de qué modo las empresas digitales utilizan técnicas basadas en la inteligencia artificial para el procesamiento de datos y el desarrollo de prácticas comerciales y publicitarias explotando los rasgos más vulnerables de los usuarios.

Consciente o inconscientemente, todos los consumidores podemos ser vulnerables a ofertas comerciales realizadas en condiciones en las que seamos un blanco fácil, ya sea por razones de necesidad (me ofrecen el producto justo en el momento en que lo necesito), de estado anímico (tengo la opción de compra justo cuando soy más propenso a celebrar el contrato) u otras circunstancias personales como la edad, religión, afinidad política u orientación sexual. Las empresas captan constantemente infinidad de datos de la más variada naturaleza a partir de los servicios y productos que a diario utilizamos, desde la navegación por Internet hasta la interacción con dispositivos conectados al Internet de las Cosas. La combinación y procesamiento de estos datos masivos de los usuarios permite inferir información con un valor muy superior al que tendrían individualmente considerados. Y esta información desempeña un papel central en la oferta de productos y servicios, en la formulación de campañas publicitarias personalizadas o en el desarrollo de innovaciones comerciales y tecnológicas que se adapten mejor a las preferencias de cada consumidor.

En las economías de mercado, la lógica que mueve el comportamiento de las empresas capitalistas es sencilla. Sus actuaciones se dirigen a la maximización del beneficio. El diseño de las estrategias para alcanzar este fin se encuentra sometido a limitaciones de distinta índole. La primera de ellas tiene carácter material y se refiere al conjunto de producción delimitado por la tecnología. Las empresas solo podrán producir dentro de su frontera de posibilidades de producción que viene determinada por la tecnología disponible en cada momento. Ésta se define como los distintos medios para obtener una cierta cantidad del producto utilizando para ello determinados factores de producción. Las diferentes tecnologías permitirán alcanzar distintos niveles de producción empleando para ello combinaciones diferentes de recursos,

normalmente cada vez a menores costes u obteniendo mayores cantidades de producto.

La segunda limitación es de naturaleza estructural. La actuación de las empresas se verá condicionada por la estructura del mercado, esto es, por las características de la demanda y la competencia que tengan del lado de la oferta. Esta clásica limitación ha sido ampliamente abordada desde la microeconomía y la teoría de la organización industrial, donde se han perfilado los contornos teóricos de los distintos modelos ideales de mercado (competencia pura, monopolio, oligopolio, competencia monopolística, etc.) y confiere el marco conceptual básico de análisis de la actuación competitiva de las empresas. Sobre esta base, se define tradicionalmente que una empresa tiene poder de mercado cuando tiene capacidad para actuar con independencia en el mismo. Es decir, una empresa tendrá poder de mercado cuando actúe como determinante de su propia conducta y los precios de sus productos y no cuando estos se consideren dados por el mercado (precio-aceptantes) ya sea por el escaso peso que la empresa tiene en la estructura general del mercado o por la reacción de la demanda.

Pero el poder de mercado puede venir modulado no solo por este factor estructural en el que normalmente se ha puesto el foco desde la economía, sino que puede ser propiciado a raíz de ciertos comportamientos oportunistas de las empresas. Para que ello ocurra es preciso alterar o falsear algunos de los postulados básicos del funcionamiento del mercado que se adoptan normalmente como punto de partida a la hora de definir los modelos económicos. Existen distintas vías para ello. Una primera opción es reducir la transparencia del mercado, de modo que desde el lado de la demanda no se tenga una información completa de la oferta y de las distintas alternativas disponibles. A resultas de ello, el oferente podrá actuar como monopolista. Se trata de una conducta próxima a la diferenciación perfecta de productos estudiada en los modelos de competencia monopolística.

Una segunda vía es la cautividad del usuario. La complementariedad de los productos y servicios digitales es mayor que la de los bienes físicos. Por ello, la estrategia de las grandes empresas digitales en los últimos años se ha dirigido a crear ecosistemas, combinando productos y servicios perfectamente conectados y que actúan como jardines vallados *(walled gardens)* para sus usuarios. Pueden elegir y moverse libremente dentro de la oferta que encuentran en el ecosistema, pero ven entorpecido el acceso a los productos situados fuera de él. Un claro ejemplo de ello ha sido la necesidad de canalizar las compras de aplicaciones móviles en los dispositivos de Apple a través de su propia tienda de aplicaciones AppStore, sin poder recurrir a la oferta competidora de otras tiendas (la Play Store de Google o la Galaxy Store de Samsung).

En este contexto, la investigación de Irene Sánchez desarrolla un análisis jurídico de las prácticas de publicidad digital personalizada basada en la elaboración de perfiles en los que se incorporan datos sensibles de los usuarios. Este análisis parte de un perfecto conocimiento del modus operandi de las empresas que operan en el sector de la publicidad digital. Estas prácticas se analizan con la combinación de una suma de regulaciones de variada naturaleza: desde los Reglamentos comunitarios de Servicios Digitales y Mercados Digitales, a las Directivas y normas nacionales sobre publicidad, competencia desleal y protección de consumidores y usuarios, pasando por la regulación de protección de datos personales. Nos encontramos ante un marco normativo complejo y que requiere un análisis cuidadoso de las conexiones y la coherencia entre normas aprobadas para fines no siempre coincidentes.

La pieza central de estudio —y punto de partida— es el análisis de la prohibición contenida en el Reglamento de Servicios Digitales de la presentación de publicidad basada en la elaboración de perfiles utilizando datos sensibles de los usuarios. Para ello, se comienza abordando la definición de qué se entiende por datos sensibles en la normativa de protección de datos y cuál es el sentido y alcance de la prohibición. En esta tarea, la autora deslinda con precisión quirúrgica las implicaciones de cada uno de los elementos de la prohibición, de modo que quede perfectamente claro qué conductas se encuentran prohibidas y cuáles, en cambio, no son alcanzadas por la prohibición. Todo ello teniendo en cuenta que nos enfrentamos a un sector, el de la publicidad digital, que se encuentra en continua y constante evolución y en el que a diario las empresas ingenian nuevas formas, cada vez más exitosas y persuasivas, de presentar sus productos.

Las empresas que operan en el mercado digital se someten a obligaciones y prohibiciones con distinto alcance en función de la naturaleza y volumen de negocios de la empresa que las ejecuta. Ello nos ha de llevar a diferenciar el ámbito obligatorio impuesto a los agentes digitales en función de si son considerados guardianes de acceso en la prestación de servicios básicos de plataforma (Reglamento de Mercados Digitales) o si son simplemente plataformas en línea en el sentido del Reglamento de Servicios Digitales. En este último contexto deberemos, igualmente, discernir si estamos ante plataformas en línea de muy gran tamaño (VLOPs), que se encuentran sometidas a obligaciones especiales.

A través de la captación masiva de información sobre los usuarios, su combinación y procesamiento, las empresas que operan en el entorno digital obtienen una información muy valiosa que utilizan estratégicamente para dirigir sus ofertas comerciales a los usuarios, sin que seamos conscientes de ello en muchos casos. Nos atacan actuando bajo una capa de invisibilidad. Muchas veces, la combinación de datos pro-

cedentes de diversas fuentes resultará especialmente peligrosa, pues, a pesar de que los datos individualmente captados no tengan la calificación de datos sensibles en el sentido de la normativa de protección de datos, al fusionarlos se puede inferir información que sí merezca esta calificación. A modo de ejemplo, los gustos manifestados por un usuario en una determinada red social no suelen constituir, por sí mismos, datos sensibles. Sin embargo, combinarlos con otra información que haya podido captar el operador digital como la edad, el sexo, sus hábitos de consumo o su historial de búsquedas en Internet, le permitirá inferir datos sensibles de este usuario como su ideología política, orientación sexual o religión.

En particular, nos interesarán los casos en que esta información inferida tenga un valor comercial o ponga de manifiesto las preferencias o necesidades de consumo del usuario. Uno de los casos más comentados es el de las empresas de alquiler de vehículos con conductor a través de una plataforma móvil (como Uber, Cabify o Bolt) que desarrollan un análisis de la zona de la ciudad en la que se encuentra el usuario, la hora del día en que solicita el servicio e, incluso, la batería que le queda en el móvil, para hacer una estimación de su «urgencia» de contratación del servicio. Si el usuario se encontrase, por ejemplo, en una zona de la ciudad especialmente aislada o peligrosa, a altas horas de la noche o tuviese el dispositivo móvil prácticamente sin batería, la empresa podría utilizar esta debilidad del usuario para ofrecerle su servicio a un precio más elevado del ordinario. Esto es, el algoritmo utilizado para la determinación del precio del servicio aplicará un precio personalizado aprovechando su situación de vulnerabilidad[5]. A medida que avanzan los sistemas de inteligencia artificial, estas prácticas se vuelven cada vez más letales y más difícilmente detectables.

En términos económicos, el operador digital cambia los presupuestos de funcionamiento de un mercado competitivo. En primer lugar, introduce opacidad en el mercado, dificultando que el usuario tenga un conocimiento completo de la oferta del mercado que le permita acudir a otras empresas. Esto se consigue, en segundo lugar, mediante la captura del usuario, levantando jardines vallados, creando efectos de ecosistema y, en suma, evitando que la demanda de este pueda ser transferida a otros oferentes. A partir de ello se consigue —en tercer lugar— el contexto adecuado en el que ejercer una nueva forma de discriminación de precios de primer grado o perfecta[6], que podemos calificar de discriminación personalizada algorítmica. Aprovechando

---

[5] Sobre este punto, el prologuista de esta obra no puede evitar recomendar al lector la consulta de la exhaustiva investigación desarrollada por Pastrana Espárraga, M., *Restricciones a la competencia mediante algoritmos en mercados digitales*, Tirant lo Blanch, Valencia, 2025.

[6] La conceptualización clásica de la discriminación de precios y sus tres categorías típicas fue desarrollada hace ya más de un siglo en la obra de Pigou, A. C., *The Economics of Welfare*, Macmillan, Londres, 1920, pp. 250 y ss., donde distingue entre discriminación de primer grado

las posibilidades de la evolución tecnológica, el uso de Big Data y de sistemas de Inteligencia Artificial con capacidad de aprendizaje autónomo, las empresas pueden estimar con precisión la disposición individual a pagar de cada consumidor o microsegmento del mercado[7], llegando —incluso— a poder predecir comportamientos o necesidades futuros. En suma, con esta forma de explotación de la vulnerabilidad de los usuarios se está actuando sobre la elasticidad estimada de la demanda individual, que permite alcanzar beneficios extraordinarios y hechos a la medida de cada contraparte en cada transacción que se celebra.

El tratamiento jurídico de estas prácticas requiere un detallado análisis de encaje de las conductas dentro de nuestra normativa sobre defensa de la competencia, competencia desleal, protección de consumidores y usuarios y protección de datos. En las páginas de esta obra se constata que se trata de una compleja labor de hermenéutica jurídica, que requiere un importante esfuerzo de desarrollo dogmático. Como el lector podrá apreciar, Irene Sánchez aborda este complejo reto con gran madurez y ofrece respuestas originales.

IV. EL CAMINO POR DELANTE

Presentadas la obra y su autora, la labor del prologuista queda prácticamente culminada. Estas líneas se escriben con el deseo de hacer justicia a la confianza depositada por su autora para acompañarla en los primeros pasos de su vida académica. En los paseos que han trazado esos pasos he querido transmitirle más preguntas que respuestas, deseando que como jurista conserve siempre el hambre ávida de pregun-

---

o perfecta, discriminación de segundo grado o por cantidades y discriminación de tercer grado o por grupos/mercados.

[7] A partir de la obra de Pigou, a finales del pasado siglo se dieron avances doctrinales destacados que permitirán un mejor entendimiento del actual fenómeno. Las primeras formas de personalización directa aprovechando la información asimétrica y que permitió el desarrollo del *screening* fueron advertidas en el sector de los seguros, lo que ofrecería una base para un nuevo análisis del fenómeno. Así, Stiglitz, J. E., «Monopoly, Non-Linear Pricing and Imperfect Information: The Insurance Market», *Review of Economic Studies*, *44*(3), 1977, pp. 407-430. A partir de este estudio, Varian, H. R., «Price Discrimination», Schlalensee y Willig, (dirs.), en *Handbook of Industrial Organization*, vol. I, Amsterdam, Elsevier, 1989, pp. 597-654, haría una reconfiguración general de la teoría de la discriminación de precios, partiendo de las clásicas categorías pigouvianas y añadiendo los nuevos avances desarrollados en el mercado. El salto a su aplicación en los mercados digitales y de plataformas lo darían Rochet, J. C. y Tirole, J., «Platform Competition in Two-Sided Markets», *Journal of the European Economic Association*, *1*(4), 2003, pp. 990-1029 y, con mayor profundidad en su revisión posterior en el artículo en *Id.*, «Two-Sided Markets: A Progress Report», *RAND Journal of Economics, 37*(3), 2006, pp. 645-667. Finalmente, de nuevo Varian, H. R., «Artificial Intelligence, Economics, and Industrial Organization», en Gans y Goldfarb (dirs.) *The Economics of Artificial Intelligence: An Agenda*, Chicago, University of Chicago Press, 2019, pp. 399-419, comenzará a hablar de la discriminación de precios *predictiva*.

tarse el porqué de las cosas y le acompañe el raciocinio para buscar soluciones jurídicas a problemas siempre nuevos.

La Universidad española no atraviesa su mejor momento (quizá nunca lo ha tenido). Y el camino, como preconizaba Platón, no será sencillo: «Gran maldad fácilmente lograrla es posible, pues llano resulta el camino y habita bien cerca del hombre; pero, en cambio, los dioses han puesto el sudor por delante de la virtud, y una ruta larga, difícil y escarpada»[8]. Nos queda, sin embargo, la esperanza de conocer una nueva generación de mercantilistas jóvenes y llenos de entusiasmo, con una loable capacidad de trabajo, que nos transmiten la confianza de que estamos en buenas manos.

Concluyo con un deseo. No solo de éxitos académicos. Estos, estoy seguro de que seguirán viniendo. Los trabajos de Irene Sánchez ya hablan por ella misma y el lector podrá comprobarlo fácilmente en las páginas que suceden. En cambio, quiero desearle —como sé que hará— que elija siempre hacer el bien, incluso cuando sus actos puedan cubrirse con la capa de invisibilidad o porte en sus dedos el anillo de Giges[9]. Y que, si alguna vez puede valerse del poder de la invisibilidad, lo haga como el héroe Perseo y no como el mezquino Gollum. Recuerda, Irene, que el injusto que obra mal sin ser descubierto o aparentando ser justo sufre un mal mayor: corrompe su alma. En cambio, el justo que realiza acciones justas, aunque reciba daño, conserva la integridad de su alma.

Comenzamos este prólogo con la historia de un anillo mágico. Desde el Egipto de los faraones los anillos se han utilizado como símbolo de unión y eternidad. Pero serían, nuevamente, los griegos clásicos los que le confirieran un valor contractual como sello para perfeccionar acuerdos. Sirva este anillo, una vez más, como prueba del compromiso asumido de acompañar a Irene en su trayectoria académica. Afrontemos tempestades o disfrutemos de plácidas travesías, siempre contarás con un puerto al que acudir.

Eugenio Olmedo Peralta

Málaga, a 15 de septiembre de 2025

Festividad de Nuestra Señora de los Dolores

(¡la del Puente!)

---

[8] Volvemos a la referencia al libro II de la *República* y al diálogo entablado entre Sócrates y Glaucón a partir de la excusa del anillo de Giges.

[9] «[…] la práctica de la Justicia es en sí misma lo mejor para el alma considerada en su esencia, y que esta ha de obrar justamente tenga o no tenga el anillo de Giges» (*ibid*.).

ABREVIATURAS

AIA	Artificial Intelligence Act (Reglamento de Inteligencia Artificial).
AMI	Asociación de Medios de Información.
BEUC	Bureau Européen des Unions de Consommateurs (Organización de Consumidores Europea)
CC	Código Civil
CCPA	California Consumer Privacy Act (Ley de Privacidad del Consumidor de California).
CEPD	Comité Europeo de Protección de Datos.
CTDPA	Connecticut Data Privacy Act (Ley de Privacidad de Connecticut).
DMA	Digital Markets Act (Reglamento de Mercados Digitales).
DPCD	Directiva sobre la Prácticas Comerciales Desleales.
DPD	Directiva de Protección de Datos.
DPEPC	Directiva sobre Publicidad Engañosa y Comparativa.
DSA	Digital Services Act (Reglamento de Servicios Digitales).
EASA	European Advertising Stardards Alliance (Alianza Europeas de Normativas Publicitarias)
EEDS	Espacio Europeo de Datos Sanitarios.
GT29	Grupo de Trabajo del Artículo 29.
IA	Inteligencia artificial.
LCD	Ley de Competencia Desleal.
LECiv	Ley de Enjuiciamiento Civil.
LGDCU	Ley General para la Defensa de los Consumidores y Usuarios
LGP	Ley General de Publicidad.
LOPJ	Ley Orgánica del Poder Judicial.
OECD	Organisation for Economic Co-operation and Develop-

	ment (Organización para la Cooperación y el Desarrollo Económico).
RGPD	Reglamento General de Protección de Datos.
TFUE	Tratado de Funcionamiento de la Unión Europea.
TJUE	Tribunal de Justicia de la Unión Europea.
UE	Unión Europea.
UWG	Gesetz gegen den unlauteren Wettbewerb (Ley alemana contra la competencia desleal).
VLOP	Very Large Online Platform (plataforma de muy gran tamaño).

INTRODUCCIÓN

La presente obra se enmarca en el proceso de transformación digital que atraviesa el mercado interior de la Unión Europea, situando su análisis en la regulación de las prácticas comerciales online basadas en perfiles, sustentadas en la explotación de datos personales y en la utilización de técnicas dirigidas a explotar vulnerabilidades de los destinatarios. La creciente sofisticación de estas prácticas plantea desafíos relevantes para la protección de los derechos fundamentales, la garantía de la libre autonomía de la voluntad de los destinatarios de servicios en línea, así como la preservación de la transparencia y la equidad en los mercados digitales.

En este contexto, el análisis de las prácticas comerciales online basadas en perfiles se vuelve imprescindible a la luz de la expansión de la economía de los datos y del papel cada vez más central que ocupan los mismos en la estructuración de las relaciones comerciales y en la configuración de los mercados digitales. La economía digital, sustentada en el tratamiento masivo de datos, da lugar a nuevas formas de poder informacional y de asimetría entre los diversos operadores económicos y los destinatarios de prácticas comerciales. Esta realidad pone de manifiesto la necesidad de examinar si los mecanismos regulatorios existentes en la Unión Europea ofrecen una protección adecuada frente a las prácticas empresariales que, mediante la explotación de datos sensibles y de vulnerabilidades individuales o grupales, afectan de manera sustancial la capacidad de decisión en los entornos digitales.

El objeto de la investigación es, por tanto, el análisis jurídico (crítico y sistemático) de las prácticas comerciales basadas en perfiles que explotan datos personales sensibles y vulnerabilidades de los usuarios, a la luz de la normativa vigente de la Unión Europea. Esta

problemática se sitúa en la intersección de varias disciplinas jurídicas, en particular el derecho de la protección de datos personales, el derecho de la competencia desleal, el derecho de las plataformas digitales y la normativa emergente sobre inteligencia artificial.

El punto de partida del análisis lo constituye una reciente prohibición establecida por el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, relativo a un mercado único de servicios (Reglamento de Servicios Digitales) (en adelante, «DSA»). En su art. 26, apartado 3, la DSA establece una prohibición específica para los prestadores de plataformas en línea consistente en no presentar anuncios basados en la elaboración de perfiles que utilicen datos personales incluidos en las categorías especiales previstas en el Reglamento (UE) 2016/679 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 (Reglamento General de Protección de Datos) (en adelante, «RGPD»).

La relevancia y novedad de esta prohibición radican en que el legislador de la UE ha optado por una prohibición absoluta sobre la presentación de publicidad basada en perfiles utilizando datos sensibles a través de plataformas online, presumiendo su carácter inaceptable y denotando un claro agnosticismo en cuanto a si dicha publicidad produce efectos positivos o adversos para los intereses individuales o colectivos.

Esta prohibición absoluta no es sino un resultado de la incesante preocupación institucional de la Unión Europea por la explotación de datos personales sensibles y vulnerabilidades con fines comerciales. La regulación contenida en la DSA constituye, sin embargo, una respuesta parcial y limitada a un fenómeno que ha demostrado ser complejo y evolutivo, como advierte un estudio de la Comisión Europea sobre el estado actual del derecho del consumo (*Fitness Check 2024*)[1], al no abordar prácticas comerciales personalizadas diferentes a la publicidad, como son la personalización de precios o el diseño adictivo de ciertos servicios digitales para condicionar el comportamiento de los destinatarios, por no mencionar la dependencia del concepto de datos sensibles, cuya operatividad actual es cada vez más discutida. Igualmente, debe advertirse que la prohibición solo resulta de aplicación a las plataformas en línea, dejando de lado otros servicios (como los videojuegos en línea) donde el fomento de vulnerabilidades comienza a alcanzar sus picos máximos.

---

[1] Whittle, M. *et al., Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161, European Commission*, 2024, p. 65.

En paralelo, el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector (Reglamento de Mercados Digitales) (en adelante, «DMA»), incorpora obligaciones específicas para los denominados guardianes de acceso, en particular la prohibición de combinar datos personales obtenidos de diferentes servicios sin el consentimiento explícito de los usuarios (art. 5, apartado 2, DMA). Sin embargo, esta depende excesivamente de modelos de consentimiento (como el conocido *pay-or-okay)* cuya legalidad resulta polémica y casuística, provocando, al igual que en la prohibición de la DSA, una dependencia (tal vez excesiva) del RGPD.

Debe advertirse, sin embargo, que la regulación de prácticas comerciales que afecten a la autonomía de la voluntad y al comportamiento de sus destinatarios no es una novedad en el marco normativo de la UE, pese a las novedades que haya podido introducir la referida prohibición de la DSA al respecto. Es más, en respuesta a las limitaciones de estas prohibiciones, el *Fitness Check 2024* subraya la importancia de acudir a una vía ya existente, que es la Directiva 2005/29/CE relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores (en adelante, DPCD), transpuesta en nuestro ordenamiento jurídico a través de la adaptación de la Ley 3/1991, de 10 de enero, de Competencia Desleal (en adelante, LCD).

El auge de la competencia desleal como vía para paliar la explotación comercial de vulnerabilidades contextualiza, asimismo, la necesidad de la presente investigación. El Tribunal de Justicia de la Unión Europea, en el caso *Lindenapotheke*[2]*,* confirmó la deseable visión conjunta entre la normativa de protección de datos y la competencia desleal como un instrumento nacional útil para reforzar los derechos de los interesados afectados por la infracción normativa. Aunque la resolución se dio a raíz de un caso alemán, guarda estrechos lazos con el ordenamiento jurídico español.

Prueba de ello es que el previsible incremento de demandas por competencia desleal debido a la infracción del RGPD ya guarda un primer precedente en España, a fecha de finalización del presente trabajo, en septiembre de 2025. Se trata de la demanda presentada por la Asociación de Medios de Información a Meta por violación de normas (art. 15 LCD) con base, precisamente, en la infracción de normativa de protección de datos con fines publicitarios. Entendiendo que entre las principales labores de la investigación jurídica se encuentran el estudio y la respuesta a conflictos emergentes aún sin resolver, tales precedentes no podían ni debían ser ignorados por esta obra, enmar-

[2] Sentencia del Tribunal de Justicia de 4 de octubre de 2024, *Lindenapotheke*, asunto C-21/23 (ECLI:EU:C:2024:846).

cada en un contexto en el que la competencia desleal por explotación comercial de datos personales cobra un creciente protagonismo.

Ahora bien, tampoco debe obviarse que el reproche de deslealtad por violación de normas necesita, inevitablemente, de una infracción normativa que no siempre resulta clara cuando la norma vulnerada es el RGPD. El dilema *pay-or-okay* es un problemático ejemplo de la creciente inseguridad jurídica en torno a la normativa europea de protección de datos y su aprovechamiento con fines comerciales.

Al hilo de esto, conviene subrayar que la Directiva de prácticas comerciales desleales (en adelante, DPCD) es señalada por el *Fitness Check 2024* como una vía para hacer frente a la explotación comercial de vulnerabilidades, particularmente en aquellos casos en los que la prohibición de la DSA no resulta de aplicación. La DPCD, que cuenta ya casi con dos décadas de edad, se ha ido revelando como un instrumento flexible para afrontar un gran número de prácticas comerciales que resultan inaceptables para el sistema de derechos y valores de la Unión. Sin embargo, esta amplia trayectoria también se traduce en la imposibilidad de haber previsto ciertas prácticas en el momento de su redacción. A título de ejemplo, la DPCD tiene en especial consideración aquellas prácticas que apelen a las vulnerabilidades de determinados grupos. Sin embargo, el actual estado de la técnica permite apelar a las vulnerabilidades concretas, sin identificar claramente a un grupo de referencia. Esta alta personalización o perfilado individual también presenta sus incógnitas para el referente del consumidor medio, hasta la fecha, entendido como aquel normalmente informado y razonablemente atento y perspicaz.

La evolución de técnicas comerciales personalizadas ha provocado, en consecuencia, inquietudes en torno a si la concepción clásica del consumidor medio continúa siendo adecuada para su propósito, las cuales se trasladaron al TJUE. En el reciente caso *Compass Banca SpA,* el Alto Tribunal mantiene este paradigma del consumidor medio, si bien admite la rebaja de los estándares señalados para aquellos casos en los que el mismo presente sesgos cognitivos, limitando su racionalidad[3]. El presente trabajo aborda la urgencia de aportar ciertas pautas (tanto generales como casuísticas) que aclaren la actual noción del consumidor medio. Con ocasión de este mismo caso, el Alto Tribunal advierte sobre la necesidad de tener en especial consideración el uso de sistemas de IA para fomentar sesgos cognitivos en determinadas prácticas comerciales.

Dicho panorama técnico justifica el encuadre de este trabajo. Los sondeos realizados por la Comisión Europea revelan que en los úl-

[3] Sentencia del Tribunal de Justicia de 14 de noviembre de 2024, asunto C-646/22*, Compass Banca SpA* (ECLI:EU:C:2024:957).

timos 5 años las técnicas subliminales basadas en IA con propósitos comerciales se han incrementado un 67,7 por ciento, acrecimiento que ha determinado la necesidad de una normativa específica al respecto[4]. Por su parte, la *Nueva Agenda del Consumidor* señaló la necesidad de tomar medidas para hacer frente a prácticas comerciales problemáticas «que ignoran el derecho de los consumidores a elegir con conocimiento de causa, abusan de sus prejuicios de comportamiento o distorsionan sus procesos de toma de decisiones»[5].

Ante este panorama, es necesario tener en especial consideración las aproximaciones realizadas en materia de prácticas comerciales personalizadas mediante sistemas de IA en el 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 (Reglamento de IA) (en adelante, AIA).

Este instrumento normativo se configura como una respuesta clave frente a los retos éticos, jurídicos y económicos generados por el uso cada vez más frecuente de sistemas inteligentes capaces de influir de manera decisiva sobre las elecciones individuales y colectivas. La AIA busca salvaguardar valores fundamentales de la Unión Europea, tales como la protección de la dignidad humana, la privacidad y la no discriminación, frente a potenciales abusos derivados del uso indiscriminado o indebido de sistemas inteligentes. Para lograrlo, establece límites claros a prácticas que resultan particularmente problemáticas desde la perspectiva de la autonomía individual y la protección de los individuos y determinados colectivos.

Entre las medidas del Reglamento se encuentra la prevención y sanción de determinadas prácticas de IA para manipular, influenciar o explotar vulnerabilidades específicas de los consumidores. Si bien no se alude expresamente a un fin comercial o publicitario, la propia AIA reconoce en sus considerandos la relación entre estas nuevas prohibiciones y la DPCD, guardando ambas, entre sus principios rectores, la protección frente a prácticas explotadoras de vulnerabilidades. Entre estas prácticas destacan el diseño adictivo de ciertos servicios (como los videojuegos o las redes sociales) o la personalización de precios en servicios de transporte.

Ante dicho contexto, la AIA busca abordar directamente estas prácticas mediante prohibiciones de determinadas prácticas de IA, como las prácticas manipulativas y subliminales, y las prácticas explotadoras de vulnerabilidades. El presente estudio se enmarca en un momento de gran inseguridad jurídica con respecto a las nuevas prohibiciones es-

---

[4] Whittle, M. *et al., Study to support the Fitness…, op. cit.,* p. 39.

[5] Comisión Europea, *Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible*, 2020.

tablecidas por la AIA, si bien encontramos dos proyectos de Directrices de la Comisión Europea sobre el concepto de sistemas de IA y sobre las prácticas de IA prohibidas que empiezan a abrir caminos más claros.

Estos proyectos de directrices subrayan que la relación de la AIA con las prácticas comerciales personalizadas es crucial, ya que estas últimas se encuentran en constante expansión debido al desarrollo tecnológico y al acceso masivo a datos personales. El uso intensivo de algoritmos predictivos, el análisis de Big Data y los sistemas de aprendizaje automático han multiplicado exponencialmente la capacidad de las empresas para influenciar las decisiones económicas de los consumidores. Sin una regulación adecuada, esta capacidad puede fácilmente derivar en abusos y formas encubiertas de explotación económica y psicológica, deteriorando el ejercicio efectivo de la autonomía de la voluntad.

En suma, la adopción de la AIA puede formularse como una respuesta al auge significativo de prácticas manipulativas, subliminales y explotadoras mediante sistemas de IA observadas en años recientes y que no irán sino en aumento. Ahora bien, la proliferación de estas prácticas evidencia la necesidad urgente de estudios e interpretaciones claras sobre la AIA que ayuden a limitar el auge de sistemas de IA que exploten comercialmente vulnerabilidades, garantizando así un mercado digital más seguro, justo y respetuoso con los derechos fundamentales.

PRIMERA PARTE

LA PROHIBICIÓN DE PRESENTAR ANUNCIOS BASADOS EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES EN LAS PLATAFORMAS EN LÍNEA. IDENTIFICACIÓN DE LAS PRINCIPALES PROBLEMÁTICAS E INTERACCIONES ENTRE LA DSA, LA DMA Y EL RGPD

CAPÍTULO I

ÁMBITO OBJETIVO DE LA PROHIBICIÓN. PRESENTAR ANUNCIOS BASADOS EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES

I. NOTAS PREVIAS SOBRE EL FUNCIONAMIENTO DE LA PUBLICIDAD *ONLINE* PERSONALIZADA

1. Categorías de publicidad *online* personalizada

En el actual entorno digital, la publicidad *online* se ha consolidado como uno de los principales pilares de financiación del ecosistema digital, articulando una compleja red de relaciones jurídicas entre múltiples actores que operan a distintos niveles. Este sistema se estructura bajo un modelo cada vez más automatizado y orientado por el uso de datos. Las transformaciones recientes del mercado, motivadas por la innovación tecnológica, el cambio en los hábitos de consumo y el refuerzo del marco normativo en materia de protección de datos y competencia han generado importantes desafíos jurídicos, cuyas implicaciones son objeto de atención tanto por parte de las autoridades nacionales como por los órganos e instituciones de la Unión Europea.

Un estudio elaborado por la Comisión Europea en 2023 destaca cómo el modelo predominante de publicidad digital se basa en la publicidad personalizada, es decir, una práctica comercial que utiliza datos sobre la actividad *online* del individuo para seleccionar qué anuncios

mostrar. Según este mismo estudio, la publicidad personalizada se clasifica en: publicidad contextual, publicidad segmentada y publicidad comportamental[1].

La publicidad contextual es un tipo de publicidad *online* personalizada que usa tecnologías incorporadas en páginas web y en aplicaciones, y que selecciona anuncios basándose en el contenido visualizado por el usuario. De esta forma, los usuarios son expuestos a anuncios que sistemas automatizados (los servidores de anuncios) han seleccionado para ellos basándose en el contenido de la página web que están visitando. Igualmente, la publicidad contextual también puede basarse en palabras clave utilizadas por el usuario en sus últimas búsquedas desde el mismo dispositivo[2].

La publicidad segmentada, por otra parte, se basa en características conocidas del usuario (tales como el sexo, la edad o la ubicación), a menudo aportadas por él mismo, principalmente, a la hora de registrarse en una página web[3]. A título de ejemplo, si un usuario revela su código postal al registrarse en una web, es probable que reciba anuncios sobre tiendas o restaurantes situados en dicha localización cuando realice búsquedas *online*[4]. Como un subtipo de publicidad segmentada, podemos encontrar también la geo-personalización, la cual se refiere al uso electrónico de la localización geográfica del usuario[5]. Esta puede incluir datos como el país, la región, la ciudad y, a menudo, el código postal. Proporciona información útil para orientar anuncios adecuados, como restaurantes cercanos. Un ejemplo conocido de orientación geográfica serían los anuncios y recomendaciones de Google basados en los datos de Google Maps, que recopilan información sobre las áreas que el usuario visita usualmente.

La publicidad comportamental, en cambio, se basa en la observación del comportamiento de los individuos durante el paso del tiempo. Su objetivo es el estudio de las características del comportamiento del usuario según sus acciones (visitas continuas a una página web, interacciones, palabras clave, publicaciones *online*…) para así desarrollar su perfil específico y ofrecerle anuncios diseñados para coincidir con sus intereses. Las empresas pueden usar esta información para determinar si un usuario pertenece a una audiencia específica a la que se dirigen, para así decidir enviarle anuncios que se adapten a su perfil[6].

---

[1] European Commission, *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*, Final Report, 2018.

[2] Eurostat. «Glossary: Internet Advertising. Statistics Explained», 2021, pp. 33-34.

[3] European Commission, *Consumer market study on online market…, op. cit.,* pp. 33-43.

[4] Lynskey, O. «Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens», *European Law Review*, 2011, pp. 874-886.

[5] Eurostat. «*Glossary: Internet Advertising…», op. cit.,* pp. 34-35.

[6] *Ibid.*, 2021.

Contrariamente a la publicidad contextual y a la publicidad segmentada (las cuales se basan en una foto o captura de lo que el individuo hace *online*, o en información que ha aportado consensuadamente), la publicidad comportamental puede trazar una imagen muy detallada del usuario sin que él mismo llegue a ser consciente de este complejo seguimiento, lo que lleva a altos dilemas éticos y jurídicos sobre esta práctica comercial.

2. Formatos en los que puede presentarse la publicidad *online* personalizada y su remuneración

La publicidad personalizada también puede ser clasificada en torno a su formato de exposición, siendo los formatos más habituales: la publicidad gráfica, la publicidad de palabras clave, la publicidad en redes sociales, la publicidad en móviles y aplicaciones, y la publicidad en *chatbots* u otros medios similares de conversación[7].

La publicidad gráfica permite a los anunciantes alcanzar determinadas audiencias basándose en las características de la página web y en los intereses de los usuarios[8]. Es comúnmente usada en la publicidad inserta en redes sociales, vídeos y *banners* publicitarios[9]. Incurre a menudo en problemas de transparencia, al basarse en insertar, reemplazar, ocultar o modificar contenido de una página web o de una aplicación[10]. Este sería el caso, por ejemplo, de los contenidos promocionados, ciertos anuncios *online* o anuncios insertos bajo la forma de publicaciones[11]. La publicidad gráfica es normalmente remunerada en torno a una base de retribución por número de impresiones, en la cual se devenga por número de visualizaciones o por el número de veces en las que un destinatario visualiza un vídeo por un mínimo de segundos o interacciona de algún otro modo estipulado[12].

Asimismo, encontramos la publicidad con palabras clave, conocida como publicidad sobre búsquedas, la cual es mostrada cuando el usua-

---

[7] European Parliament, Directorate-General For Internal Policies Of The Union, Sartor, G., Lagioia, F., Galli, F., *Regulating targeted and behavioural advertising in digital services: how to ensure users' informed consent*, European Parliament, 2021, pp. 22-52.

[8] Adam, A., Halls, S. y Ryan, A., «Changing digital advertising landscape – overview of EU and UK competition cases and regulatory initiatives», *European Competition Law Review*, 43(5), 2022, pp. 209-218.

[9] European Parliament, Directorate-General for Internal Policies of the Union, Lognoul, M., Hill, J., Godlovitch, I. *et al.*, *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice, European Parliament*, 2021, pp. 16-26.

[10] Vivero De Porras, C. «Publicidad ilícita por vía electrónica como acto de competencia desleal: publicidad personalizada en Instagram», *Actas de Derecho Industrial*, 2023, pp. 57-58.

[11] European Parliament, Directorate-General for Internal Policies of the Union, Sartor, G., Lagioia, F., Galli, F., *Regulating targeted and behavioural…, op. cit.,* pp. 22-52.

[12] Adam, A., Halls, S. y Ryan, A. «*Changing digital advertising landscape…», op. cit.*

rio utiliza herramientas de búsqueda *online*. En este contexto, los anuncios comerciales se presentan en posiciones destacadas, generalmente por encima o junto a los resultados obtenidos, siendo seleccionados a través de mecanismos de subasta automatizada que operan en función de las palabras clave introducidas por el usuario en su consulta. Este tipo de publicidad se basa normalmente en un modelo de remuneración por clic, en virtud del cual el anunciante únicamente debe abonar una tarifa cuando el usuario interactúa efectivamente con el anuncio, accediendo al contenido promocionado mediante un clic[13]. En este modelo publicitario, la dependencia de datos personales del usuario es, por lo general, reducida, en la medida en que la selección de los anuncios se determina principalmente por la consulta de búsqueda específica realizada por el usuario, y no tanto por datos individuales o perfiles previamente elaborados[14]. Sin embargo, en algunos casos, los datos personales se pueden utilizar para respaldar el proceso de coincidencia[15].

La publicidad sobre búsquedas o palabras clave constituye una de las modalidades publicitarias que presentan mayores niveles de eficiencia desde la perspectiva de la tasa de conversión, entendida esta como el porcentaje de usuarios que, tras haber visualizado un anuncio, realizan la acción deseada, consistente, en este caso, en hacer clic sobre dicho anuncio, en relación con el número total de usuarios expuestos al mismo[16]. La elevada eficacia de esta modalidad publicitaria se debe a que permite alcanzar a los consumidores en un momento en el que se encuentran en disposición de adoptar una decisión de compra, habida cuenta de que han manifestado activamente su interés mediante la realización de una consulta específica relativa al producto o servicio en cuestión a través de un motor de búsqueda[17]. En Estados Unidos y Europa, este segmento está fuertemente dominado por Google y su servicio Google Ads[18].

Por otra parte, también es distinguible la publicidad a través de redes sociales. Dichos sitios web son el entorno perfecto para la publicidad personalizada, teniendo en cuenta la cantidad de tiempo que los usuarios pasan navegando por ellos. En las redes sociales, la orientación puede basarse no solo en el historial de navegación, sino también en los

---

[13] European Parliament, Directorate-General for Internal Policies of the Union *et al.*, *Online advertising: the impact…», op. cit.*

[14] Adam, A., Halls, S. y Ryan, A. «*Changing digital advertising landscape…», op. cit.*

[15] CMA, *Online platforms and digital advertising, Market study final report*, 1 de julio 2020, pp. 42-68.

[16] European Parliament, Directorate-General for Internal Policies of the Union *et al.*, *Online advertising: the impact…», op. cit.*

[17] Geradin, D. y Katsifis, D., «An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age», *TILEC Discussion Paper No. DP2019-031*, 12 de diciembre de 2018.

[18] European Parliament, Directorate-General for Internal Policies of the Union *et al.*, *Online advertising: the impact…», op. cit.*

datos de comportamiento recopilados en la plataforma (características sociodemográficas, seguidores, me gusta y otras acciones). Al aplicar análisis de *big data* sobre dicha información, se han desarrollado formas nuevas y más intensas de personalización de contenido. Estas redes sociales permiten a los especialistas en publicidad aprovechar la capacidad de influencia de los usuarios, ya sea directamente (por ejemplo, a través de influencers) o indirectamente (difusión de vídeos virales) al crear, compartir y distribuir contenido a través de redes de amigos, seguidores y otros contactos[19]. A través de técnicas de personalización, programas como la «Audiencia personalizada» de Facebook o el «Administrador de audiencia» de Google permiten a los especialistas en marketing preseleccionar rasgos específicos del consumidor, como la ubicación, la demografía, sus intereses y comportamiento[20].

Por su parte, la publicidad móvil (es decir, la publicidad optimizada para formatos de teléfono móvil) capacita la provisión de diferentes contenidos, como banners, publicidad en vídeos, en pantalla completa y opciones gamificadas e interactivas. La publicidad móvil puede encontrarse tanto en páginas web como en aplicaciones, y aprovecha las oportunidades que ofrecen los dispositivos móviles para recopilar y utilizar datos en tiempo real basados en la ubicación del usuario (la llamada «orientación geográfica»), como los favoritos de las compras y las páginas web frecuentadas. Por lo general, se entrega a través de la intermediación de propietarios de plataformas móviles (por ejemplo, Apple iAd y AdMob de Google) o tiendas de aplicaciones, que actúan como redes publicitarias móviles. Estas redes proporcionan plataformas técnicas para publicar anuncios, ofrecer herramientas de desarrollo de anuncios, motores de orientación y servidores de anuncios. Además, las redes publicitarias móviles agregan el espacio publicitario de los editores, vendiéndolo a los especialistas en marketing y plataformas del lado de la demanda[21].

Por último, otra forma de proveer publicidad personalizada es a través de *chatbots* y la denominada publicidad conversacional, originada por innovaciones relativamente recientes en la tecnología. A través de los chatbots, es posible ofrecer publicidad personalizada en tiempo real. Algunos de estos mecanismos son bastante conocidos: no solo los chatbots —normalmente usados para atención al cliente en páginas web—, sino también a través de relojes inteligentes y otros accesorios portátiles, o a través de altavoces inteligentes —como Alexa o Siri—. Todos estos nuevos dispositivos están basados en el uso de tecnología IA.

---

[19] European Parliament, Directorate-General for Internal Policies of the Union *et al.*, *Online advertising: the impact…», op. cit.*

[20] European Parliament, Directorate-General for Internal Policies of the Union, Sartor, G., Lagioia, F., Galli, F., *Regulating targeted and behavioural…, op. cit.,* pp. 22-52.

[21] *Ibid.*

En el estado actual de la ciencia, las utilidades publicitarias de la mayoría de los dispositivos mencionados anteriormente aún son limitadas, ya que los algoritmos por los cuales funcionan no son tan ajustables a situaciones fuera de cánones como sus creadores desearían. Los *chatbots* son un buen ejemplo de esto: cuando el cliente hace una pregunta que no está contemplada en el algoritmo del *chatbot*, falla y proporciona una respuesta inútil que no está relacionada en absoluto con la pregunta.

Como es común en la industria publicitaria, las distinciones no siempre están claras, y las empresas pueden operar a través de diversos modos de publicidad digital[22].

II. ACTORES EN LA PUBLICIDAD DIGITAL

Este modelo, denominado publicidad basada en el comportamiento (*behavioral advertising*), ha suscitado preocupaciones crecientes desde una perspectiva jurídica, no solo por sus implicaciones sobre los derechos fundamentales (como el honor, la intimidad, la protección de datos personales o la no discriminación), sino también por el impacto que genera sobre la competencia, la pluralidad informativa y la sostenibilidad del modelo económico de los medios de comunicación. A juicio de la Comisión, la situación actual se caracteriza por una concentración excesiva de poder en manos de un número muy reducido de empresas tecnológicas, fenómeno que puede distorsionar la competencia en el mercado y debilitar la capacidad de negociación de operadores de menor tamaño.

Desde una perspectiva estructural, el mercado publicitario digital puede ser descrito como una cadena de valor en la que intervienen distintos sujetos con roles específicos. En primer lugar, encontramos los anunciantes, es decir, aquellos operadores económicos que contratan espacios publicitarios con el fin de promocionar sus productos, servicios o marcas. Su actuación puede ser directa o mediante agencias de medios, que gestionan y optimizan sus campañas.

En el extremo opuesto se sitúan los editores, es decir, los titulares de sitios web, aplicaciones móviles u otras plataformas digitales que ponen a disposición sus espacios para la inserción de anuncios a cambio de una retribución económica. Entre ambos extremos, se inserta una pluralidad de intermediarios tecnológicos, cuyas funciones consisten en facilitar la compraventa automatizada de espacios publicitarios mediante tecnologías como las plataformas de demanda (*demand-side platforms*), plataformas de oferta (*supply-side platforms*) y mercados de puja (*ad*

[22] Adam, A., Halls, S. y Ryan, A. «*Changing digital advertising landscape…», op. cit.*

exchanges). A esta red se suman también los denominados data brokers o intermediarios de datos, que recogen, agregan y comercializan perfiles de usuarios para su utilización con fines comerciales.

Uno de los rasgos más relevantes del sistema es la existencia de plataformas integradas verticalmente, que operan de forma simultánea en varias fases del proceso. Este es el caso paradigmático de Alphabet, que actúa como proveedor de servicios publicitarios, como plataforma de intermediación y como editor, generando múltiples conflictos de interés que han sido objeto de investigaciones por parte de autoridades de competencia tanto a nivel europeo como nacional. De hecho, el estudio de la CNMC publicado en 2021 subraya que Google y Meta concentran conjuntamente más del 70 por ciento de la inversión publicitaria digital en España, ejerciendo un notable poder de mercado sobre los demás operadores. Esta situación ha dado lugar a preocupaciones sobre la falta de transparencia en los mecanismos de subasta de espacios publicitarios, la dificultad de los anunciantes y editores para verificar el retorno de la inversión, y la posibilidad de prácticas discriminatorias en la gestión del inventario publicitario.

III. CONTEXTO Y JUSTIFICACIÓN DE LA PROHIBICIÓN DE PRESENTAR ANUNCIOS BASADOS EN PERFILES QUE UTILICEN DATOS SENSIBLES

La regulación del uso de datos personales con fines publicitarios es uno de los grandes retos a los que se enfrenta la Unión Europea en las últimas décadas. Este reto se diseña como una suerte de cubo de Rubik, donde la convergencia de diversos intereses nos sitúa ante un rompecabezas permanentemente desordenado. En una cara del cubo encontramos el objetivo de crear un marco adecuado para el avance tecnológico. Para facilitar la innovación, el legislador comunitario debe integrar múltiples piezas en esta cara del acervo de la UE, facilitando el acceso, la transferencia, el análisis y la interoperabilidad de los datos, una de las prioridades de la UE dentro de su estrategia «Una Europa adaptada a la era digital»[23]. Esta cara del rompecabezas se complementa con otra, la libertad de empresa. El valor de los datos deriva de la versatilidad de los usos que se pueden hacer de ellos. La creación de mensajes publicitarios personalizados a partir del tratamiento de datos es una de las actividades más lucrativas que se pueden desarrollar en este ámbito. Por ello, muchos proveedores de servicios digitales han adaptado su modelo de negocio a la publicidad personalizada y a la monetización de datos personales, optando por políticas de priva-

[23] European Commission, «Political guidelines of the European Commission 2019-2024».

cidad y condiciones generales que les sean ventajosas en atención al creciente valor que puede extraerse de estos datos[24].

El orden de estas piezas jamás permanece inalterado, ya que los anteriores colores del cubo de Rubik —avance tecnológico y libertad de empresa— se ven continuamente entremezclados con la entrada en juego de otros intereses. Entre ellos, destacan los fines de defensa de la competencia y la necesidad de promover que el mercado de la publicidad digital funcione siguiendo dinámicas competitivas[25]. Es necesario cuestionar, en este marco, si las grandes plataformas deberían compartir datos entre ellas sin limitación alguna. La solución del rompecabezas se topa también con la necesidad de ordenar la cara opuesta: garantizar un nivel adecuado de protección de los sujetos a los que se refieren los datos. El tratamiento de datos personales con fines de publicidad personalizada puede derivar en grandes riesgos para los derechos fundamentales de los ciudadanos, tales como el derecho a la privacidad, a la protección de datos y a la no discriminación[26].

En este último extremo, el foco de atención se ha puesto sobre un tipo concreto de publicidad: la basada en la elaboración de perfiles utilizando categorías especiales de datos, conocidos como «datos sensibles». El uso publicitario de estos genera riesgos significativos para los derechos fundamentales de los individuos, al permitir presentar de forma discriminatoria anuncios que afecten a la igualdad de trato y oportunidades de los ciudadanos[27]. Como señalan los considerandos de la DSA, de la presentación de anuncios basados en técnicas de segmentación optimizadas para responder a intereses de los destinatarios y apelar potencialmente a sus vulnerabilidades[28] pueden derivar efectos jurídicos especialmente severos. En algunos casos, las técnicas de manipulación pueden afectar negativamente a intereses de colectivos concretos contribuyendo a aumentar los perjuicios sociales. También resultarán de singular relevancia las actuaciones en desarrollo de cam-

---

[24] Frosio, G. y Geiger, C. «Taking fundamental rights seriously in the Digital Services Act's platforms liability regime», *European Law Journal*, vol. 29, 2023 pp. 59.67.

[25] Rodilla Martí, C. «Problemas de defensa de la competencia en el mercado de la publicidad online», *Tax legal advisory review: La revista para el mundo económico-empresarial*, núm. 3, 2022, pp. 23-25; Rodilla Martí, C. «Los mercados de plataformas digitales: entre el derecho de la competencia y la regulación», *Revista General de Derecho de los Sectores Regulados: RSR*, núm. 8, 2021; Ruiz Peris, J. I. «The EU digital markets act, a european answer to application's problems of classical competition law to Gatekeepers», en Ruiz Peris, J. I. (dir.), *Competencia, compensación de daños y mercados digitales*, 2022, pp. 17-53.

[26] Lynskey, O. «*Track[ing] changes: an examination…», op. cit.,* pp. 874-886.

[27] Tomassi, S. «Digital Services and algorithmic discrimination», en *The risk of discrimination in the Digital Market. From the Digital Services Act to the future*, Springer, 2022, pp. 37-50.

[28] Si bien la vulnerabilidad no es un concepto abordado por la DSA, cabe reseñar el paralelismo subyacente entre este concepto y la explotación de datos sensibles, paralelismo al que nos referiremos en posteriores apartados de este trabajo.

pañas de desinformación o que impliquen la discriminación de ciertos grupos sociales[29].

Por estas razones, la Comisión Europea decidió integrar una nueva prohibición en el marco normativo de la UE a través de la DSA, aplicable desde el 17 de febrero de 2024[30]. El art. 26.3 de la DSA señala que «los prestadores de plataformas en línea no presentarán a los destinatarios del servicio anuncios basados en la elaboración de perfiles, tal como se define en el art. 4, punto 4, del Reglamento (UE) 2016/679, utilizando las categorías especiales de datos personales a que se refiere el art. 9, apartado 1, del Reglamento (UE) 2016/679». Conforme a dicha formulación, los caracteres del ámbito objetivo de la prohibición serían los que siguen:

1) La actividad prohibida es «presentar» el tipo de publicidad descrita.
2) El término «anuncio» o publicidad debe ser entendido conforme a la definición propia que aporta la DSA.
3) La publicidad prohibida debe estar basada en la elaboración de perfiles, término definido por remisión al RGPD.
4) No deben utilizarse «categorías especiales de datos», también entendidas como datos sensibles, para cuya definición la norma se remite al RGPD.

Seguidamente pasaremos a analizar cada uno de estos aspectos.

IV. LA ACTIVIDAD PROHIBIDA: «PRESENTAR» PUBLICIDAD BASADA EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES

Conforme a la formulación de la norma, la actividad prohibida es presentar publicidad basada en la elaboración de perfiles utilizando datos sensibles. Teniendo en cuenta la amplitud del término «presentar», el protagonismo parece situarse en el rol de la plataforma como servicio de intermediación, en este caso, como medio publicitario en el que insertar anuncios basados en la elaboración de perfiles.

Sin embargo, la dicción de la norma puede resultar un tanto confusa, al recoger que los prestadores de plataformas en línea «no presentarán» a los destinatarios del servicio anuncios basados en la elaboración de perfiles a partir de categorías especiales de datos personales. La versión inglesa plantea las mismas dudas, al emplear la terminología *shall not present,* y lo mismo sucede con la francesa, bajo la dicción *ne pré-*

[29] Considerando 68 DSA.

[30] Conforme al art. 93. 2 DSA, salvo ciertos apartados (entre los que no se incluye la prohibición), la totalidad del Reglamento resulta aplicable desde el 17 de febrero de 2024.

sentent pas. Se nos plantea la duda, vista esta dicción, de si la prohibición de utilizar datos personales sensibles recae sobre: *a)* la forma de presentación o segmentación de dichos anuncios, *b)* el contenido de los propios anuncios, o *c)* ambos extremos.

Comencemos por el primer uso, es decir, el acto de presentar el anuncio. Conforme a una interpretación contextual de la DSA, el foco de la prohibición no parece situarse en el contenido del anuncio, sino en su forma de presentación o, más concretamente, en la selección de sus destinatarios (*targeting*)[31]. El considerando 68 de la DSA, al exponer la *rationale* de la prohibición, alude a «la presentación discriminatoria de anuncios», que no, por ejemplo, a anuncios con contenido discriminatorio, por lo que el protagonismo parece situarse en la forma de seleccionar a los destinatarios. De igual forma, el art. 26 de la DSA, en el que se inserta la prohibición, se centra en la regulación de aspectos relativos a la transparencia de los anuncios —como el acceso a información acerca de los parámetros utilizados para determinar al destinatario— pero no se refiere al contenido sustantivo del anuncio. Así, apuntan acertadamente algunos autores que la DSA muestra más preocupación por el proceso y el diseño de los servicios de intermediación que por el contenido en sí[32]. Por otro lado, si la cuestión a examinar fuese la licitud del contenido sustantivo, ya encontramos en la DSA y demás normativa aplicable otras obligaciones de diligencia impuestas a las plataformas sobre este extremo[33].

Bajo esta interpretación, si analizamos el contenido sustantivo del anuncio, habrá que atender, en principio, a las disposiciones de diligencia debida sobre contenidos ilícitos en las plataformas, mientras que, para la selección de los destinatarios de dichos anuncios (*targeting*), habrá que atender a la prohibición del art. 26.3 de la DSA[34].

---

[31] Teniendo en cuenta, además, que el contenido suele determinarse por el anunciante o un tercero —no por la propia plataforma—, toda vez que el ámbito subjetivo de la prohibición solo abarca a estas últimas.

[32] Husovec, M. y Roche Laguna, I. «Digital Services Act: A Short Primer», *SSRN Electronic Journal*, 2022.

[33] Entre otros, encontramos los mecanismos de notificación y acción del art. 16 DSA, o el sistema interno de gestión de reclamaciones regulado por el art. 20 DSA. En este punto, conviene destacar que la ilicitud de los contenidos puede obedecer a múltiples causas, no reduciéndose solo a infracciones de derechos de autor y a otros contenidos normalmente vetados expresamente en las plataformas, como el discurso de odio, el acoso o la pornografía infantil. La ilicitud podrá obedecer a cualquier infracción de normas imperativas, incluidas las de consumo y protección de datos, ya que el art. 3.*h)* de la DSA define como contenido ilícito como toda información que incumpla el derecho de la Unión o el derecho de cualquier Estado miembro que cumpla el derecho de la Unión, sea cual sea el objeto o carácter concreto de ese derecho aunque, conforme a ciertos estudios, la causa más común de retirada de contenidos *online* sea la infracción de derechos de autor. Por todos, *vid.* Peukert, A. *et al.*, «Comment on Copyright and the Digital Services Act Proposal», *IIC – International Review of Intellectual Property and Competition Law*, 53(3), 2022, p. 358-376.

[34] De esta forma, si el contenido del anuncio muestra, por ejemplo, productos falsificados, resultará de aplicación la normativa referente a contenidos ilícitos de DSA, además de otras disposiciones nacionales y comunitarias aplicables, como aquellas relativas al derecho de marcas.

Pese a esta interpretación, se aprecian casos en los que determinados parámetros de la presentación del anuncio (como el formato, su diseño o el precio aplicado) son determinados mediante el uso de algoritmos. Este tratamiento automatizado utiliza perfiles basados en datos sensibles para ofrecer diferentes outputs, consiguiendo la mejor consecución posible del objetivo perseguido. Es decir, aunque la prohibición se imponga subjetivamente a los proveedores de servicios de plataforma, y normalmente el contenido sea determinado por terceros —anunciantes y agencias de publicidad— las plataformas no siempre actúan como meras intermediarias, sino que inciden activamente en la configuración del mensaje publicitario. De este modo, no son pocas las ocasiones en las que el algoritmo de la plataforma ejerce también cierta influencia sobre el contenido del anuncio.

Este sería el caso de los servicios que utilizan algoritmos basados en la optimización dinámica de material creativo (como Amazon Ads). Estos algoritmos son entrenados para crear en tiempo real varias versiones de un anuncio utilizando la misma plantilla, adaptando partes componentes del mensaje en función de las audiencias, el contexto y el rendimiento anterior[35]. Un ejemplo podría ser la presentación de anuncios *online* sobre contratos de seguro de vida. Utilizando sistemas DCO, ciertas partes del anuncio, como el precio del seguro, pueden adaptarse al destinatario en tiempo real conforme a categorías de datos sensibles, como datos relativos a la salud[36].

En la misma situación se encuentra otra plataforma publicitaria dominante, Google Ads, que reconoce utilizar sistemas de IA generativa para crear y adaptar anuncios de búsqueda de manera más efectiva en función del contexto de una consulta. La propia empresa muestra un ejemplo de ello a través de su web. Con una búsqueda de «cuidado de la piel para piel seca y sensible», la IA de Google Ads puede usar el contenido de una *landing page* y los anuncios existentes para crear un nuevo título que se alinee aún más con la consulta, como «Suaviza tu piel seca y sensible»[37]. En casos como este, Google Ads no solo sirve como medio para publicitar el producto, sino que también ayuda a seleccionar destinatarios relevantes para el mismo y a modificar el propio anuncio para que resulte más efectivo.

Utilizando sistemas como los anteriores, parece evidente que la línea divisoria entre la elaboración del contenido del anuncio y la

---

[35] Información ofrecida por la web de Amazon Ads. disponible en *https://advertising.amazon.com/es-es/library/guides/dco-dynamic-creative-optimization.*

[36] Como comentaremos más adelante, este fenómeno, conocido como personalización o discriminación de precios, plantea también ciertas preocupaciones en el ámbito del derecho de la competencia desleal. Por todos, *vid.* Louredo Casado, L. «El posible carácter desleal e injusto de los precios personalizados en internet», *Derecho Digital e Innovación. Digital Law and Innovation Review,* núm. 7, 2020.

[37] Dischler, J. «Una nueva era de Google Ads impulsada por Inteligencia Artificial». 2023.

selección de sus destinatarios es bastante difusa, ya que ciertas partes del anuncio se diseñan en tiempo real conforme al perfil del destinatario. La doctrina ya había discutido un fenómeno similar en sede de protección de datos, describiendo algunos autores que las fases de: *a)* elaboración de perfiles y *b)* toma de decisiones (como la aplicación de perfiles) tienden a solaparse, ya que pueden concurrir coetáneamente[38]. A efectos prácticos, se nos plantea la duda de si el uso de datos sensibles para adaptar elementos del anuncio quedaría igualmente prohibido bajo la DSA.

En este sentido, si volvemos a la literalidad de la norma, la actividad prohibida es presentar «anuncios basados en la elaboración de perfiles […] utilizando las categorías especiales de datos»[39]. En consecuencia, cabe interpretar que el ámbito objetivo de la prohibición abarca no solo la utilización de datos sensibles para la presentación de los anuncios, sino también para el diseño de su contenido a partir de los perfiles de usuarios inferidos para fines publicitarios[40]. Siguiendo el ejemplo anterior, el ajuste del precio del contrato anunciado conforme a datos sensibles sería claramente una consecuencia directa del tratamiento automatizado con fines evaluativos de dichos datos.

Para precisar si la prohibición de usar datos sensibles se limita solo a la selección de los destinatarios o si se aplica también a la determinación de elementos del propio anuncio, utilizaremos la sencilla aproximación de la separabilidad de actuaciones. En síntesis, se trataría de determinar si ambos actos pueden separarse materialmente en conductas independientes con sentido por sí mismas. Fácilmente se comprobará que la respuesta ha de ser negativa. Siempre que se personalizan elementos del anuncio opera también la selección o *targeting* de los destinatarios. Dicho de otro modo, no tendría sentido alguno afirmar que el contenido se personaliza sin tener en cuenta las características del destinatario al que va dirigido. Esta afirmación iría en contra del mismo sentido del *targeting*, ya que necesariamente debe existir una correlación o *matching* entre el anuncio y el destinatario cuando nos referimos a la publicidad basada en perfiles.

Cabría concluir, por ende, que la prohibición opera sobre cualquier tipo de publicidad basada en perfiles utilizando datos sensibles, inde-

---

[38] Por todos, *vid.* Wuiedemann, K. «Profiling and (automated) decision-making under the GDPR: A two-step approach», *Computer Law & Security Review*, 45, 2022, pp.14-16.

[39] Art. 26.3 DSA.

[40] En este sentido, el concepto de elaboración de perfiles, como veremos más adelante, es bastante amplio, al comprender «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física» (art. 4.4 RGPD). El RGPD pone como ejemplo de evaluación de rasgos personales el análisis o la predicción de aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona física.

pendientemente de si el propio contenido ha sido personalizado o no. Por ello, para que la prohibición resulte aplicable, basta con que el destinatario sea seleccionado teniendo en cuenta datos sensibles, no siendo esencial que el contenido en sí mismo sea personalizado en tiempo real para el destinatario concreto. Cerrando con el ejemplo anterior: pongamos el caso de que solo se utilice un mismo modelo de anuncio sobre contratos de seguro, pero este anuncio solo se dirija a destinatarios que manifiesten unos ciertos caracteres relativos a la salud, como, por ejemplo, una determinada enfermedad. Este tipo de anuncio quedaría prohibido por la norma de la DSA, ya que estaría basado en la elaboración de perfiles, al haberse escogido su destinatario conforme a la aplicación de un perfil basado en datos personales sensibles.

V. LA REFORMULACIÓN DEL TÉRMINO «ANUNCIO» O «PUBLICIDAD», EN LA DSA. EXCLUSIÓN DE PRÁCTICAS PERSONALIZADAS QUE NO SEAN PUBLICIDAD

1. Análisis comparado del concepto de publicidad en la normativa de la UE, la normativa nacional y la DSA

El segundo requisito para que concurra el ámbito objetivo de la prohibición es que el anuncio o publicidad se ajuste a la definición propia de publicidad que ofrece la DSA. En este sentido, es evidente que el texto oficial en castellano de la DSA ofrece una traducción poco rigurosa de su primera redacción en lengua inglesa. El art. 26 de la DSA se refiere a «anuncios» basados en la elaboración de perfiles utilizando datos sensibles, pero en ningún momento la norma define el término anuncio, sino que el concepto definido es «publicidad». Aunque ambos términos puedan ser considerados sinónimos, hubiera resultado deseable que la traducción española optase por utilizar en todo el articulado el mismo término, «publicidad», teniendo además en cuenta que la DSA aporta una reformulación importante del concepto que podría pasar inadvertida al lector poco familiarizado con la materia. En cambio, la versión original inglesa muestra una mayor coherencia léxica, al emplear en el art. 26 el término *advertising* tanto para referirse a la publicidad prohibida como al definir qué debemos entender por *advertising* en el art. 3.*r)*. Lo mismo sucede en la versión francesa, al utilizar en ambos artículos el mismo término: *publicité.* Por tanto, en este caso la imprecisión de la traducción no es general de la versión del texto en lenguas romances, sino exclusivamente de la española.

Traducciones discutibles aparte, lo más reseñable radica en la reformulación del concepto de publicidad. En la normativa de la UE previa a la entrada en vigor de la DSA, la publicidad se describe como concep-

to general en la Directiva sobre Publicidad Engañosa y Comparativa[41] (en adelante, DPEPC) como «toda forma de comunicación realizada en el marco de una actividad comercial, industrial, artesanal o liberal con el fin de promover el suministro de bienes o la prestación de servicios, incluidos los bienes inmuebles, los derechos y las obligaciones», limitándose al ámbito B2B[42].

Por su propio ámbito, la Directiva sobre Prácticas Comerciales Desleales (en adelante, «DPCD») se refiere a la publicidad en tanto que práctica comercial dentro de su ámbito de actuación. Así, se consideran prácticas comerciales «todo acto, omisión, conducta o manifestación, o comunicación comercial, *incluidas la publicidad* y la comercialización, procedente de un comerciante y directamente relacionado con la promoción, la venta o el suministro de un producto a los consumidores»[43]. En este caso, el ámbito subjetivo de la norma no son ya las relaciones interempresariales (B2B), sino entre empresario y consumidor (B2C)[44]. Naturalmente, la noción de práctica comercial es mucho más amplia que la de publicidad, que simplemente es una manifestación concreta de esta. Lo mismo se desprende de la jurisprudencia del TJUE, el cual ha reconocido como prácticas comerciales:

— La publicidad, incluyendo en esta el uso de un nombre de dominio y el de metaetiquetas (*metatags*) en los metadatos de un sitio web, pero no el registro de un nombre de dominio[45].
— Ofrecer a los consumidores la posibilidad de ganar un premio en juegos, rompecabezas o concursos con el objeto de persuadirles para que compren un determinado producto[46].
— Las ofertas combinadas, incluyendo aquellos tipos de ofertas combinadas en las que uno de los componentes ofrecidos es un servicio financiero[47].

---

[41] Directiva 2006/114/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, sobre publicidad engañosa y publicidad comparativa, en adelante DPEPC).

[42] Artículo 2.*a)* DPEPC.

[43] La cursiva es nuestra.

[44] *Vid.* Art. 2.*d)* de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior.

[45] Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de marzo de 2013, *Euronics Belgium CVBA contra Kamera Express BV y Kamera Express Belgium BVBA*, asunto C-343/12 (ECLI:EU:C:2013:154).

[46] Sentencia del Tribunal de Justicia de la Unión Europea, de 26 de junio de 1997, *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH contra Heinrich Bauer Verlag*, asunto C-368/95 (ECLI:EU:C:1997:325).

[47] Sentencia del Tribunal de Justicia de la Unión Europea, de 23 de abril de 2009*, VTB-VAB NV contra Total Belgium NV y Galatea BVBA contra Sanoma Magazines Belgium NV*, asuntos acumulados C-261/07 y C-299/07 (ECLI:EU:C:2009:244); Sentencia del Tribunal de

— La venta a pérdida como medio de persuadir a los consumidores para que realicen una transacción comercial[48].

Si bien la DPEPC y la DPCD se diferencian por su ámbito de aplicación personal (B2B y B2C, respectivamente), el denominador común de ambas, al definir los conceptos de publicidad y práctica comercial, es la concurrencia de los siguientes elementos: *a)* una conexión con la empresa o actividad comercial[49]; y *b)* el objetivo de promover la contratación de bienes o servicios[50]. Señala así Massaguer que las actuaciones comprendidas en la DPCD son singularizadas por un aspecto funcional: su relación directa con la promoción, venta o suministro de bienes o servicios[51]. Diversas normas nacionales de los Estados miembros, al definir el concepto de publicidad, requieren la concurrencia de uno o ambos de los citados elementos.

A nivel nacional, la Ley General de Publicidad (en adelante, «LGP») define la publicidad como «toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, industrial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de bienes muebles o inmuebles, servicios, derechos y obligaciones»[52]. En esta definición se recogen ambos elementos: la conexión con el comercio (expresada aquí como «el ejercicio de una actividad comercial») y el objetivo de promover las ventas de bienes o servicios.

En derecho comparado encontramos otras soluciones. Así, el Código Belga de Derecho Económico define la publicidad como « toda comunicación que tenga por objeto directo o indirecto la promoción de la venta de productos, independientemente del lugar o medio de comunicación utilizado»[53]. En este caso, solo se recoge expresamente el segundo elemento, es decir, que el objetivo sea la promoción de ventas.

Justicia de la Unión Europea, de 18 de julio de 2013, *Citroën Belux NV contra Federatie voor Verzekerings- en Financiële Tussenpersonen (FvF),* asunto C-265/12 (ECLI:EU:C:2013:498).

[48] Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de marzo de 2013*, Euronics Belgium CVBA contra Kamera Express BV y Kamera Express Belgium BVBA*, asunto C-343/12 (ECLI:EU:C:2013:154).

[49] En la DPEC, esta conexión es expresada al aludir a aquella forma de comunicación «realizada en el marco de una actividad comercial, industrial, artesanal o liberal» y en la DPCD se hace referencia a que el acto debe ser «procedente de un comerciante».

[50] En la DPEC este objetivo es recogido al exigir que la comunicación debe realizarse «con el fin de promover el suministro de bienes o la prestación de servicios, incluidos los bienes inmuebles, los derechos y las obligaciones», y en la DPCD se exige que el acto esté «directamente relacionado con la promoción, la venta o el suministro de un producto a los consumidores».

[51] Massaguer Fuentes, J. *El nuevo derecho contra la competencia desleal. La Directiva 2005/29/CE sobre las prácticas comerciales desleales*, Thomson Civitas, 2006, pp. 17-30.

[52] Art. 2 LGP.

[53] Artículo I. 8. 131/4, capítulo 3, del Código Belga de Derecho Económico (*Code de droit Économique*).

En la normativa alemana no existe una definición específica de publicidad, pero sí de práctica comercial, la cual se define en su Ley contra la Competencia Desleal como «cualquier forma de comunicación destinada a promover la venta de bienes, servicios o derechos»[54]. En este caso, concurre igualmente solo el segundo elemento: el objetivo de promocionar ventas.

Tampoco existe una definición legal específica de publicidad en la normativa austríaca. Nuevamente solo encontramos un concepto de «actividad comercial», definida en su Ley contra la Competencia Desleal como «cualquier comportamiento de una persona a favor de la propia empresa o de la empresa de otro, antes, durante o después de un negocio, y que esté directamente relacionado con la promoción de la venta o compra de bienes o servicios o con la celebración o ejecución de un contrato de bienes o servicios que esté objetivamente relacionado»[55]. En esta definición concurren ambos elementos: la conexión con un comercio o empresa —en este caso, la norma se refiere de una forma amplia al *comportamiento a favor de la empresa propia o ajena*—, y el propósito de promocionar ventas.

En la normativa italiana se define la publicidad como «cualquier forma de mensaje que se difunda, de cualquier forma, en el ejercicio de una actividad comercial, industrial, artesanal o profesional con el fin de promover la transmisión de bienes muebles o inmuebles, la prestación de obras o servicios o el establecimiento o cesión de derechos y obligaciones que les imponen»[56]. Concurren, por tanto, ambos elementos: la conexión comercial y el propósito de promoción de ventas[57].

En la normativa francesa la publicidad es definida como «cualquier forma de mensaje televisado difundido a cambio de una remuneración

---

[54] Núm. § 2, apartado para. 1, punto 2, de la Ley alemana contra la competencia desleal (*Gesetz gegen den unlauteren Wettbewerb* – en adelante, UWG).

[55] Núm. § 1, apartado para. 4, punto 2, de la Ley Federal Austríaca contra la Competencia Desleal (*Bundesgesetz gegen den unlauteren Wettbewerb* – UWG).

[56] Art. 2.*a)* del Decreto Legislativo italiano del 2 de agosto de 2007, núm. 145/2007 (*Decreto Legislativo 2 agosto 2007, núm. 145, Attuazione dell'articolo 14 della Direttiva 2005/29/CE che modifica la direttiva 84/450/CEE sulla pubblicità ingannevole*).

[57] Ambos factores se vienen incluyendo de largo en la normativa publicitaria italiana, formulada de una forma amplia para acoger un amplio espectro de comunicaciones en el concepto de publicidad. La exigencia de una finalidad promocional y una conexión con el comercio, así como esta amplia formulación, se encontraba ya en el art. 2.*a)* del Decreto Legislativo italiano de 25 de enero de 1992, núm. 74 (*Decreto Legislativo 25 gennaio 1992, n.°74, Attuazione della direttiva 84/450/CEE, come modificata dalla direttiva 97/55/CE in materia di pubblicità ingannevole e comparativa*). En el mismo se definía ya la publicidad como «cualquier forma de mensaje que se difunda, por cualquier medio, en el ejercicio de una actividad comercial, industrial, artesanal o profesional, con el propósito de promover la venta de bienes muebles o inmuebles, la constitución o la transmisión de derechos y obligaciones sobre los mismos, o bien la prestación de obras o servicios». Para un análisis este concepto en la normativa italiana, *vid.* Fernández Carballo-Calero, P. I. «Concetto e caratteri generali», en Fernández Carballo-Calero, P. I. *Pubblicità occulta e product placement,* Cedam, 2024, p. 3-6.

u otra compensación con el fin de promover el suministro de bienes o servicios, incluidos los presentados bajo su nombre genérico, en el marco de una actividad comercial, industrial, artesanal o profesional, o para garantizar la promoción comercial de una empresa pública o privada»[58]. Concurren igualmente ambos elementos, aunque la definición se constriñe a la difusión televisiva y requiere, como requisito adicional, que la difusión se lleve a cabo a cambio de una remuneración.

La normativa griega, por su parte, define la publicidad en su Ley de Protección del Consumidor como «todo anuncio realizado por cualquier medio en el contexto de fines comerciales, industriales, actividad manufacturera o profesional con el objetivo de promover la disponibilidad de bienes o servicios, incluidos los bienes inmuebles y los derechos y obligaciones conexos»[59]. Esta definición recoge ambos elementos: la conexión con el comercio y la promoción de ventas de bienes, aunque se refiera a la *disponibilidad de bienes* en una traducción literal.

Menos expresiva, la normativa de consumidores de la República de Irlanda indica en su Ley de Protección del Consumidor que la publicidad incluye «cualquier forma de anuncios o marketing»[60], sin proporcionar definiciones de estos conceptos.

Los países escandinavos no ofrecen una definición legal específica de publicidad. Así, en Dinamarca no se define la publicidad, pero sí se incluye el concepto al definir las prácticas comerciales, entendidas por la Ley Danesa de Prácticas de Comercialización como «todo acto, omisión, conducta o manifestación, o comunicación comercial, incluidas la publicidad y la comercialización, procedente de un comerciante y directamente relacionado con la promoción, la venta o el suministro de un producto a los consumidores»[61]. Esta definición es una transposición *verbatim* de la DPCD, en la cual se requiere la concurrencia de ambos elementos: el elemento comercial y el objetivo de promocionar ventas.

Como último ejemplo, en la normativa sueca, el concepto más similar podría ser el marketing, que se define en la Ley Sueca de Comercialización como «anuncios y otras medidas tomadas en el curso de los negocios con el fin de promover las ventas y la disponibi-

---

[58] Artículo 2 del Decreto francés núm. 92-280 de 27 de marzo de 1992 relativo a la publicidad y patrocinio audiovisual (*Décret n.° 92-280 du 27 mars 1992 relatif à la publicité et au parrainage audiovisuels*).

[59] Artículo 9. 1) *a)* de la Ley griega núm. 2251/1994 de Protección del Consumidor (Νόμος 2251/1994, Προστασία των καταναλωτών).

[60] Artículo 2, punto 1, de la Ley de la República de Irlanda de Protección del Consumidor de 2007 (*Consumer Protection Act 2007*).

[61] Artículo 2, párrafo 1, punto 4, de la Ley Danesa de Prácticas de Comercialización (*Bekendtgørelse af lov om markedsføring*).

lidad de productos»[62]. Concurren ambos elementos: la conexión con un comercio o empresa, al referirse a *medidas tomadas en el curso de los negocios*, y el propósito de promover ventas.

De esta comparativa se concluye que existe una tendencia en la normativa anterior a la DSA a exigir que la información, para ser considerada publicidad, tenga: *a)* una conexión con el comercio, empresa o similar, y/o *b)* el objetivo de promover la contratación de bienes y servicios. En otras palabras, tanto en la normativa de la UE como en la de los Estados miembros se exige un elemento comercial para que la normativa de publicidad resulte de aplicación.

El concepto de publicidad experimenta una completa reformulación a partir de la DSA. La información o el mensaje transmitido no tiene por qué presentar ninguno de los anteriores elementos, ya que el art. 3.*r)* de la DSA define el término publicidad como «la información diseñada para promocionar el mensaje de una persona física o jurídica, con independencia de si trata de alcanzar fines comerciales o no comerciales, y presentada por una plataforma en línea en su interfaz en línea a cambio de una remuneración específica por la promoción de esa información». En otras palabras, conforme a la DSA, la finalidad o el contenido de la información resulta irrelevante para que esta sea calificada como publicidad. El carácter definitorio lo marca la transmisión de un mensaje a cambio de una remuneración a la plataforma por la promoción de un mensaje, remuneración que puede ser directa o indirecta[63].

Ahora bien, esta definición se acota a los mensajes transmitidos por los servicios de plataforma en línea, y no a los otros servicios de intermediación regulados en la DSA. Se excluyen, por tanto, los servicios de mera transmisión y memoria caché. Esta acotación subjetiva se confirma bajo una visión contextual, ya que las obligaciones de la DSA relativas a la publicidad solo se aplican a los prestadores de plataformas en línea, como bien indica el art. 26 y su encuadre en la sección tercera del capítulo II, titulada «Disposiciones adicionales aplicables a los prestadores de plataformas en línea».

El hecho de que la norma no requiera a la plataforma una finalidad comercial para calificar su actividad de publicitaria puede parecer baladí, pero tiene relevantes implicaciones. La amplitud del nuevo concepto implica, por ejemplo, que mensajes sin fines comerciales claros, como los transmitidos por las ONG o la propaganda política, sean conside-

[62] Artículo 3 de la Ley sueca de Comercialización (*Marknadsföringslagen*).

[63] Husovec, M. y Roche Laguna, I. «Digital Services Act…», *op. cit.*; y considerando 68 DSA.

rados publicidad a efectos de la DSA[64]. En el ámbito de la publicidad política, esta inclusión refleja una reciente tendencia comunitaria a paliar mensajes que manipulen la información y las decisiones electorales de los ciudadanos, a raíz del escándalo de *Cambridge Analytica*. Una de las principales consecuencias de esta reformulación es que las comunicaciones políticas presentadas por servicios de plataforma deberán cumplir con las obligaciones de la DSA referentes a la publicidad. Así, entre otros extremos, no podrán basarse en perfiles elaborados con datos sensibles, y deberán cumplir con ciertos requisitos de transparencia, como la accesibilidad a los parámetros utilizados para determinar a los destinatarios[65].

Pese a las evidentes ventajas que puede plantear la formulación amplia del concepto de publicidad en la DSA, tampoco podemos pasar por alto que, paralelamente, se excluye de la misma a ciertas prácticas personalizadas que pueden resultar problemáticas por la explotación de datos sensibles o vulnerabilidades. Así, por amplia que resulte la reformulación del concepto de publicidad, este sigue extendiéndose exclusivamente a aquella información destinada a promover un mensaje. El concepto de publicidad no cubre la discriminación o personalización de precios. Estas son otras prácticas comerciales —desleales en su caso—, pero que no están relacionadas con la presentación del mensaje publicitario.

2. Interacciones con el Reglamento sobre transparencia y segmentación en la publicidad política

Es reseñable que esta amplitud del concepto de publicidad bajo la DSA cierra filas con el Reglamento sobre transparencia y segmentación en la publicidad política[66]. Conforme a su art. 3.2), la publicidad política también se formula como un concepto extenso, al comprender «la preparación, inserción, promoción, publicación, entrega o difusión, por cualquier medio, de un mensaje, normalmente prestada a cambio de una remuneración o mediante actividades internas o como parte de una campaña de publicidad política:

a) por un actor político, en su nombre o por su cuenta, a menos que sea de carácter estrictamente privado o estrictamente comercial, o

b) que pueda influir en el resultado de unas elecciones o un referéndum, en el comportamiento electoral o en un proceso legislativo

---

[64] Duivenvoorde, B. y Goanta, C. «The regulation of digital advertising under the DSA: A critical assessment», *Computer Law & Security Review*, 51, 2023, pp. 5-6.

[65] *Vid.* Art. 26 DSA.

[66] Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política. En adelante, Reglamento de Publicidad Política.

o reglamentario, a nivel de la Unión, nacional, regional o local, y esté diseñada para ello».

La segunda casuística —letra *b)*— es la que claramente marca la amplitud del concepto, englobando prácticas de *micro-targeting* que quedaban insuficientemente cubiertas por el RGPD[67-68]. En lo que aquí nos atañe, un denominador común entre este Reglamento y la DSA es la prohibición de usar datos sensibles con fines de publicidad basada en perfiles. Así, el art. 18.1.*c)* del Reglamento de Publicidad Política indica que no estarán permitidas las técnicas de segmentación o las técnicas de entrega de anuncios que impliquen el tratamiento de datos personales en el contexto de la publicidad política en línea cuando dichas técnicas impliquen la elaboración de perfiles[69] utilizando datos sensibles[70]. Al igual que en la DSA, los dos componentes fundamentales de esta prohibición son: *a)* la elaboración de perfiles publicitarios utilizando datos sensibles, entendida esta como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física[71], y *b)* la utilización de datos sensibles[72].

Bajo la DSA, la actividad prohibida consiste en presentar cierto tipo de publicidad, mientras que, bajo este Reglamento, las actividades prohibidas son determinadas técnicas de segmentación y de presentación de anuncios con finalidad política[73]. Diferencias terminológicas aparte, bajo una interpretación teleológica, la *rationale* de ambas prohibiciones parece ser la misma: evitar que los datos sensibles se utilicen con fines de publicidad basada en perfiles.

---

[67] Dobber, T. Ó; Fathaigh, R. y Zuiderveen Borgesius, F. J. «The regulation of online political micro-targeting in Europe», *Internet Policy Review*, 8(4), 2019, versión online.

[68] Aunque no sea el objeto de este trabajo, a nuestro juicio, la amplitud y subjetividad del apartado *b)* podría ser excesiva, ya que existe una miríada de mensajes o información que puede ser susceptibles de afectar el comportamiento electoral de los ciudadanos, ya sea de forma directa, ya sea de forma subliminar.

[69] Tal como se define en el art. 4.4 del RGPD y en el art. 3.5 del Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

[70] En el sentido del artículo 9.1 RGPD y el artículo 10.1, del Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

[71] Art. 4.4) RGPD.

[72] Art. 9.1 RGPD.

[73] El considerando (6) del Reglamento de Publicidad Política define las técnicas de segmentación como «aquellas técnicas que se utilizan para dirigir un anuncio político únicamente a una persona o un grupo de personas específicos o para excluirlos, generalmente con contenido personalizado, sobre la base del tratamiento de datos personales». Igualmente, también define las técnicas de entrega de anuncios «como una amplia gama de técnicas de optimización que se basan en el tratamiento automatizado de datos personales para aumentar la circulación, el alcance o la visibilidad de un anuncio político».

La diferencia más reseñable entre ambas prohibiciones radica, a nuestro entender, en el ámbito subjetivo. Así, la aplicación personal del Reglamento de Publicidad Política es mucho más amplia que la de la DSA, ya que se refiere a cualquier proveedor de publicidad política, independientemente de si es o no una plataforma *online*[74]. Consideramos que esta es una de las principales ventajas del Reglamento de Publicidad Política en lo referente a la publicidad personalizada. Como indicábamos, la publicidad política estaría englobada dentro del concepto de publicidad de la DSA, por lo que no debería basarse en la elaboración de perfiles utilizando datos sensibles. Sin embargo, esta prohibición de la DSA solo se aplica a los prestadores de plataformas en línea y, en consecuencia, otros servicios quedarían excluidos. Esta carencia, como indicamos, se salva gracias a la prohibición del Reglamento de Publicidad Política, ya que su ámbito personal cubre a cualquier prestador de servicios de publicidad política, independientemente de si esta se presenta o no en una plataforma en línea.

En conclusión, a efectos de la DSA, es conveniente no perder de vista que es innecesaria la concurrencia de un objetivo comercial en la publicidad; basta con que el mensaje se presente a cambio de una remuneración específica, ya sea directa o indirecta. La principal consecuencia de la amplitud de esta reformulación del término «publicidad» es que engloba todo mensaje transmitido a través de dicha remuneración, por lo que todo mensaje transmitido en una plataforma a cambio de una remuneración deberá cumplir con los requisitos de la DSA. Ahora bien, según sus caracteres —como es el caso de la publicidad política— el mensaje en cuestión puede estar sujeto a obligaciones adicionales.

VI. LA PUBLICIDAD BASADA EN «LA ELABORACIÓN DE PERFILES»

El tercer requisito para que la publicidad en cuestión quede sujeta a la prohibición es que esté basada en la *elaboración de perfiles*. Al concretar qué ha de entenderse por tal, se vuelve a poner de manifiesto la dependencia e interrelación entre la DSA y el RGPD. Así, la conceptualización de la elaboración de perfiles se hace por remisión al art. 4.4 del RGPD, que lo caracteriza como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física»[75]. El precepto aporta un listado abierto de aspectos evaluables bajo la elaboración de perfiles, incluyendo parámetros como el rendimiento profesional, situación económica, salud, preferencias persona-

[74] Art.1.1. del Reglamento de Publicidad Política.
[75] Art. 4.4) RGPD.

les, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. Existe, por tanto, una infinidad de caracteres a los que se pueden referir los datos que se tomen en consideración para la elaboración de perfiles, especialmente cuando se traten para fines publicitarios. La norma aclara también que la evaluación comprende tanto el análisis como la predicción de tales aspectos, lo cual —como veremos en apartados posteriores— es ya un indicador de que los datos inferidos quedan abarcados por la evaluación de perfiles.

1. El uso de medios automatizados para la elaboración de perfiles: algoritmos, análisis de *big data* e inteligencia artificial

El RGPD exige que la elaboración de perfiles se lleve a cabo mediante un tratamiento automatizado, si bien en ningún momento aporta una definición de este último término. El Grupo de Trabajo del Artículo 29 (en adelante, «GT29»), precursor del actual Comité Europeo de Protección de Datos (en adelante, «CEPD»), aclara que es un tipo de tratamiento en el que la posible intervención humana no implica necesariamente que el procesamiento deje de ser automatizado[76]. El evidente propósito de esta aclaración es evitar que una eventual y mínima intervención humana, de apenas relevancia, evite la aplicación de ciertas obligaciones adicionales para el responsable de datos cuando las decisiones se basen en tratamientos automatizados[77].

La utilización de instrumentos automatizados para el tratamiento de datos resulta esencial para la elaboración de perfiles publicitarios en la publicidad *online*[78]. Los algoritmos son el instrumento básico utilizado para ello. Estos pueden ser definidos como una secuencia ordenada y finita de instrucciones que ha de ser aplicada a un número finito de datos para llevar a cabo una tarea específica[79]. En contextos publicitarios, los algoritmos pueden presentar diferentes funcionalidades, siendo las principales: *a)* aglutinar a diferentes sujetos (algoritmos

---

[76] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017.

[77] Un ejemplo de decisión individual automatizada sería el *credit scoring*, es decir, la generación automatizada de un valor de probabilidad a partir de datos personales relativos a una persona y acerca de la capacidad de esta para hacer frente a compromisos de pago en el futuro, como señala la Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de diciembre de 2023, *OQ contra Land Hessen*, asunto C-634/21 (ECLI:EU:C:2023:957).

[78] Ebers, M. y Sein, K., «Data-driven Technologies – Challenges for Privacy and EU Data Protection Law» in Ebers, M. y Sein, K. P*rivacy, Data Protection and Data-driven Technologies*, Routledge, 2024, pp. 16-23.

[79] Robles Martín-Laborda, A. «Cuando el cartelista es un robot. Colusión en mercados digitales mediante algoritmos de precios», *Actas de Derecho Industrial y Derecho de Autor*, 2018, p. 4.

de agrupamiento); *b)* conocer los hábitos y comportamientos de los sujetos (algoritmos de clasificación); y *c)* predecir mediante pronósticos basados en datos objetivos (algoritmos de regresión)[80].

El siguiente nivel en la sofisticación de las técnicas para el procesamiento automatizado de datos es el uso de *Big Data Analytics*, o análisis de *big data*. El *big data* ha sido definido como un conjunto vasto de datos sobre diversas actividades de personas, máquinas o datos derivados del entorno, que pueden ser utilizados para diversos fines[81]. El análisis de *big data*, por su parte, se refiere a una tecnología que permite buscar, recolectar y comparar enormes cantidades de datos mediante un procesamiento informático[82]. Es recurrente en la doctrina la alusión a la *definición V3* del *big data*, destacando los rasgos de su variedad, velocidad y volumen[83]. El análisis de *big data* aplicado a la elaboración de perfiles publicitarios permite adaptar en tiempo real tanto los destinatarios del anuncio como, en ocasiones, el propio contenido del anuncio con base a una plantilla.

Con el actual estado de la técnica, la aplicación de los sistemas de IA es la que permite una mayor personalización de la actividad publicitaria consiguiendo inferir los rasgos esenciales de cada usuario a partir de los datos obtenidos respecto a él. Con ello se logra optimizar la actividad publicitaria, consiguiendo que el mensaje (y sus costes) se dirija a aquellos usuarios en los que es más probable obtener una reacción efectiva. En otras palabras, se maximiza la rentabilidad de la inversión en publicidad.

Tras el desarrollo, durante casi una década, de un cálido debate para definir la IA, el Reglamento de Inteligencia Artificial (en adelante, AIA) finalmente adoptó una definición normativa a nivel de la UE, identificándolo como «un sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales»[84]. Como tendremos ocasión de analizar más adelante, la mayoría de sistemas publicitarios utilizados en la actualidad para la elaboración de perfiles

---

[80] Núñez Seoane, J. «El derecho de la información y acceso al funcionamiento de los algoritmos que tratan datos personales», en Huergo Lora, A. *La regulación de los algoritmos*, Thomson Reuters Aranzadi, 2020, pp. 299-315.

[81] Kupčík, J. y Mikeš, S. «Discussion on big data, online advertising and competition policy», *European Competition Law Review*, 2018.

[82] Ništevic, *Profiling through Big Data Analytics*, Intersentia, 2023, pp. 91-107.

[83] Braganza, A. «The Challenges of Artificial Intelligence», *International Corporate Rescue*, 15(2), 2018,p.114.

[84] Art. 3 (1) del Reglamento de Inteligencia Artificial.

se basan en el uso de complejos sistemas de IA, que quedan dentro del ámbito de aplicación del AIA.

2. Tipos de perfiles englobados en la prohibición

No sería trivial plantearnos si la elaboración de perfiles a la que se refiere la DSA comprende tanto los perfiles individuales como los perfiles grupales, ya que el concepto de elaboración de perfiles del RGPD, al que se remite, presenta un carácter considerablemente amplio. Así, se viene señalando que la elaboración de perfiles puede dirigirse hacia: *a)* un individuo en particular o *b)* hacia un individuo como parte de un grupo predeterminado[85].

La elaboración de perfiles individuales (a la que la normativa también se refiere como elaboración de perfiles personales) es la que toma como referencia a un solo sujeto individualmente considerado, que es caracterizado por una serie de atributos. A través de la minería aplicada a diversas fuentes de datos, el algoritmo puede ser entrenado para recolectar información sobre los hábitos y rutinas del individuo, correlacionar dicha información y construir el perfil individual del sujeto. De esta forma, no hay un perfil predeterminado en el que se encasille al sujeto, sino que el perfil se diseña y aplica para el sujeto concreto.

En cambio, en la elaboración de perfiles grupales se toma como referencia a un colectivo predeterminado, en el cual sus miembros comparten una serie de características comunes, si bien estos individuos pueden ser divididos en subcategorías[86]. Conforme a los perfiles grupales, el algoritmo publicitario será entrenado para dirigir el anuncio hacia los individuos que presenten las características de ese grupo predefinido. A pesar de esta distinción, la noción de elaboración de perfiles que utiliza el RGPD cubre ambas categorías. Tanto en los perfiles individuales como en los grupales se tratan de forma automatizada datos personales para evaluar aspectos de una persona física, ya se entienda o no a esta como parte de un colectivo mayor. La diferencia principal puede radicar en que, en el caso de los perfiles grupales, se distinguen más claramente las fases de: *a)* elaboración del perfil y *b)* aplicación del perfil. En cambio, en los perfiles individuales estas fases tienden a solaparse[87].

Siguiendo una interpretación contextual, se ha de entender que la prohibición de la DSA se extiende tanto a los perfiles individuales

---

[85] Nišević, M. *Profiling through Big Data…, op. cit.,* pp. 91-107.

[86] *Ibid.*, pp. 91-107.

[87] Petkova, B. y Boehm, F. «Profiling and the Essence of the Right to Data Protection» in Selinger, E., Polonetsky, J. y Tene, O. *The Cambridge Handbook of Consumer Privacy,* Cambridge University Press, 2018, pp. 185-300.

como a los grupales[88]. Esta interpretación se deriva del considerando 69 de la norma, en el cual se señala que se prohíbe presentar anuncios: *a)* basados en la elaboración de perfiles utilizando datos sensibles o *b)* basados en la elaboración de perfiles basados en categorías de perfiles que usen datos sensibles. Con la primera alusión entendemos que se refiere a los perfiles individuales, es decir, perfiles dependientes de las características individuales de cada sujeto. La segunda mención —perfiles basados en categorías de perfiles—, en cambio, engloba también a los perfiles grupales o perfiles predeterminados. Bajo una interpretación contextual se entiende que el legislador ha querido incluir tanto los perfiles creados para cada individuo en concreto como los perfiles grupales, aplicados a cada individuo conforme a las afinidades que presente para ser encuadrado en un grupo predeterminado o en varios de ellos.

Cabe plantearnos, por otro lado, las razones por las que la DSA no ha optado por introducir literalmente una prohibición total de la elaboración de perfiles utilizando datos sensibles. Recordamos que el supuesto de hecho prohibido por la DSA es la presentación de publicidad basada en perfiles utilizando datos sensibles o, en otras palabras, utilizar los perfiles basados en datos sensibles con fines publicitarios. Esta acotación se debe, a nuestro entender, a que los perfiles basados en datos sensibles son un arma de doble filo.

El primer filo, que es el que fundamentaría una prohibición total de la elaboración de perfiles basados en datos sensibles, es el que podríamos denominar «filo del riesgo», seguido por muchos sectores pro-privacidad. Es decir, este filo atiende a los riesgos que presenta esta práctica, sin incorporar en la aproximación por riesgo la probabilidad de que se produzca un perjuicio, bastando con una posibilidad remota. Algunos autores opinan que la elaboración de perfiles tiene un potencial excesivamente dañino, aunque no se lleguen a tomar decisiones basadas en ellos[89]. Para sectores en la doctrina más tendentes a priorizar la privacidad de los individuos frente a otros intereses, la prohibición de la DSA resultaría insuficiente, ya que no se prohíbe que las plataformas puedan elaborar perfiles conforme a datos sensibles de sus usuarios, sino que lo que se prohíbe es solamente que emitan publicidad basada en dichos perfiles. Nada impide taxativamente que se utilicen estos perfiles con otros fines —como la personalización de contenidos— o los moneticen al transmitirlos a terceros, siempre que concurra una base legal válida. El actual modelo de bases legales del RGPD provoca un profundo pesimismo en el

---

[88] *Cfr.* Considerando 69 DSA.

[89] Savin, A. «Profiling in the Present and New EU Data Protection Frameworks» in Nielsen, P. A., Schmidt, P. K., Dyppel Weber, K. *Erhvervsretlige emne, Juridisk Institut CBS,* Djøf Forlag, 2015, pp. 249-270.

Farrel, J. «Can privacy be just another good?», *Journal on Telecommunications and High Technology Law*, 2012.

sector del consumo, en el cual —con cierta razón— se tiende a considerar que nos encontramos ante un grave «desequilibrio disfuncional», en el que los individuos han perdido el control sobre sus datos personales, convertidos en un mero bien comerciable[90].

El segundo filo justificaría la tendencia a liberalizar la elaboración de perfiles basados en datos sensibles. Nos podríamos referir a él como «filo de la innovación». Esta acotación se debe, a nuestro entender, a las ventajas que pueden obtenerse a partir de la elaboración de perfiles. Entre estos usos positivos podemos encontrar, por ejemplo en el ámbito sanitario, el uso primario de datos sobre salud para el tratamiento de pacientes, o el uso secundario para la elaboración y aplicación de perfiles de pacientes tendentes a sufrir ciertas enfermedades, con el objetivo de detectar tales enfermedades tempranamente o incluso prevenirlas[91]. El interés público que puede plantear la recolección y transmisión de datos sensibles en campos I+D lleva a que ciertos autores afirmen la necesidad de tratar jurídicamente dichos datos como una propiedad o bien colectivo[92].

Sin embargo, es conveniente precisar que las actuales vías legislativas para fomentar la transmisión de datos, incluidos los sensibles, conllevan normalmente como medida de seguridad la anonimización de tales datos, cuando sea posible, y, cuando no, su seudoanonimización[93]. En el caso de la seudoanonimización, seguiría aplicándose la normativa de protección de datos. En cambio, si los datos son anonimizados, perderán el carácter de datos personales, por lo que escaparían del ámbito prohibitivo de la normativa[94].

La anonimización no es posible —ni guardaría sentido alguno— en el ámbito de la publicidad basada en perfiles, ya que necesariamente los perfiles serán aplicados a individuos concretos, por lo que los datos tendrán el carácter de datos personales. En consecuencia, la normativa de protección de datos resultará de aplicación íntegra e imperativamente. En otras palabras, la aplicación de perfiles no es otra forma más de tratamiento de datos personales sujeta al RGPD, al dirigirse a sujetos

---

[90] *Ibid.*, pp.6-10.

[91] García Álvarez, P. «Aplicación de redes neuronales en la predicción de mortalidad por neumonía», *Scielo*, 2020.

[92] Zimmer, D. «Property rights regarding data?» in Lohsse, S., Schulze, R. y Stardenmayer, D. *Trading data in the digital economy: legal concepts and tools*, Nomos, 2017, pp. 101-133.

[93] Entre estas vías cabe destacar el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 (en adelante, EEDS).

[94] Wendehorst, C. «Of elephants in the room and paper tigers: how to reconcile data protection in data economy» in Lohsse, S., Schulze, R. y Stardenmayer, D. *Trading data in the digital economy…, op. cit.,* pp. 327-357.

de datos identificados o identificables[95]. En el caso de la elaboración de perfiles con fines publicitarios, el argumento del interés público tendría poca cabida, ya que en la misma entran en juego otros intereses, como el derecho a la libertad de empresa esgrimido por la plataforma y el derecho a la privacidad de sus usuarios, definido por ciertos autores como «el derecho a que nos dejen en paz» *(the right to be left alone)*[96].

Como dicha anonimización no es posible en el ámbito de la publicidad personalizada, la elaboración de perfiles publicitarios usando datos sensibles puede entrañar evidentes riesgos en cuanto a la privacidad y el derecho a la no discriminación de los ciudadanos. Este sería el caso de los perfiles publicitarios elaborados con datos relativos a la salud, si son utilizados por parte de compañías aseguradoras para personalizar los precios anunciados o excluir a determinados individuos de campañas publicitarias, ejemplo que lleva ya un tiempo advirtiéndose[97].

Pese a los posibles riesgos que pueda presentar la elaboración de perfiles utilizando datos sensibles, ciertos sectores, con los cuales esta autora se encuentra de acuerdo, consideran que la solución no debe pasar por prohibir radicalmente esta práctica. La elaboración de perfiles puede ser positiva e incluso necesaria en innumerables casos, desde el punto de vista del interés tanto social como individual. En ciertos ámbitos tecnológicos, científicos y comerciales, la posibilidad de acceder y utilizar estos perfiles resulta crítica para la innovación y el desarrollo de nuevos modelos de negocio. En otras palabras, si se prohibiese la elaboración de perfiles sobre bases sensibles, se estarían vetando no solo sus usos negativos sino también los positivos. Por esta razón, consideramos que la solución debe ser proporcionada y su aplicación ha de ser diferenciada en función de la fase del proceso ante la que nos encontremos.

En la fase previa, durante la cual se produce la recolección y el análisis de datos personales para la elaboración de perfiles conforme a ellos, resultaría necesario introducir medidas para garantizar que el consentimiento que los usuarios prestan a que sus datos sean procesados sea libre[98]. Asimismo, en esta fase previa es esencial implementar estrictos requisitos de transparencia para asegurar la explicabilidad de las decisiones tomadas por el algoritmo, incluyendo los datos utilizados y los

---

[95] En el mismo sentido se pronuncia Castillo Parrilla, J.A. «Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial», *Derecho Privado y Constitución*, 43, 2023, pp. 53-88.

[96] Entre los autores más pioneros y representativos de esta argumentación encontramos a Lawrence Lessig, que ya incluía la misma en Lessig, L. «The code of Privacy», *Proceedings of the American Philosophical Society*, vol. 151, 2007.

[97] Wachter, S. «Affinity profiling and discrimination by association in online behavioral advertising», *Berkeley Technology Law Journal*, vol. 35, núm. 2, 2020, pp. 369-392.

[98] En el mismo sentido se pronuncian otros autores. *Vid.*, por todos, Ebers, M. y Sein, K., «Data-driven Technologies…», *op. cit.,* pp. 16-23.

parámetros empleados para llegar a una decisión o a otra[99]. Es decir, debe asegurarse que haya una trazabilidad respecto a si los datos tratados son datos personales, si tienen el carácter de sensibles, y por qué el algoritmo decide, por ejemplo, dirigir el anuncio a un destinatario y no a otro, o por qué el precio es mayor para determinados destinatarios.

VII. LA UTILIZACIÓN DE «CATEGORÍAS ESPECIALES DE DATOS PERSONALES», EN LA PUBLICIDAD BASADA EN PERFILES. LA REMISIÓN AL RGPD Y SU PRIMACÍA COMO NORMA DE CONFLICTO

El último requisito para que se aplique la prohibición del art. 26.3 de la DSA es que se hayan utilizado categorías especiales de datos personales —también denominados datos sensibles— para la presentación de publicidad basada en perfiles. Según el razonamiento que hemos mantenido anteriormente, se ha de entender que la norma abarca el uso de datos sensibles tanto para seleccionar a los destinatarios del anuncio como para personalizar los elementos del anuncio en sí (como el formato, diseño o precio ofertado) conforme al perfil del destinatario.

Lo más reseñable de este último requisito es que, para la definición de los datos sensibles, el art. 26.3 de la DSA se remite al art. 9.1 del RGPD. En esta norma se define a los datos sensibles como todos aquellos «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física».

Esta remisión no es sino otra manifestación de la posición de primacía que otorga el legislador comunitario al RGPD en todo lo referente a la regulación de los datos personales. Esta primacía se aprecia no solo en la DSA, sino también en el resto de normas encuadradas en la política de la Comisión Europea denominada «Una Europa adaptada a la Era Digital»[100]. El Consejo de la Unión Europea ya recalcó en noviembre de 2023 que cualquier norma nueva que contuviese previsiones relativas al tratamiento de datos debía ser consistente con el RGPD y la jurisprudencia del TJUE[101].

---

[99] Sobre este punto, *vid.* Senftleben, M. «Trademark Law, AI-Driven Behavioural Advertising and the Digital Services Act – Towards Source and Parameter Transparency for Consumers, Brand Owners and Competitors» in Cheltenham, *Research Handbook on Intellectual Property and Artificial Intelligence*, Edward Elgar, 2022.

[100] European Commission, «Political guidelines of the European…», *op. cit.*

[101] Council Of The European Union, «Council position and findings on the application of the General Data Protection Regulation (GDPR), 15507/23», 2023, § 40.

Consecuentemente, los cinco reglamentos encuadrados en esta estrategia, sin excepción, reconocen la primacía del RGPD en todo lo referente al tratamiento de datos personales, si bien la formulación empleada para reconocer dicha preferencia varía ligeramente de una norma a otra[102]:

— La DSA, la DGA y el Reglamento de Datos establecen que sus normas operan *sin perjuicio de* la legislación de la UE en materia de protección de datos personales, todos ellos haciendo expresa referencia al RGPD[103].

— La DMA incluye una redacción similar, al señalar que se aplica *sin perjuicio del RGPD*, si bien tal preferencia solo se llega a reconocer expresamente en uno de sus considerandos y no en el cuerpo imperativo de la norma[104]. El art. 1, que define su ámbito de aplicación, incluye referencias a otras normas que tienen prioridad sobre la DMA, pero entre ellas no menciona al RGPD. Sin embargo, la primacía del RGPD sí que queda manifiesta de forma concreta en ciertas obligaciones de la norma. Como veremos más adelante, la remisión al RGPD resulta de gran relevancia al prohibir en su art. 5(2) ciertas prácticas a los guardianes de acceso y establecer como excepción el consentimiento del sujeto de datos en virtud del RGPD[105]. Igualmente, el art. 8 de la DMA señala que el guardián de acceso garantizará que la aplicación de esas medidas sea conforme con el derecho aplicable, en particular, con el RGPD.

— El Reglamento de IA también define la relación entre el mismo y el RGPD, pero utiliza un lenguaje más evasivo, señalando en su art. 2 (7) que la norma *no afectará al RGPD*. Tanto el CEPD como el SEPD señalaron la necesidad de evitar divergencias entre ambas normas, recomendando igualmente que los sistemas de IA de alto riesgo deberían contener un sistema de verificación de cumplimiento con el RGPD[106], si bien el Reglamento de IA no ha llegado a incluir obligaciones específicas al respecto. Los considerandos del reglamento se limitan a señalar

---

[102] Zanfir-Fortuna, G. «Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's "Fit for the Digital Age" Legislative Package», *EDPS at 20 Anniversary Volume*, 2024, pp.7-16.

[103] Art. 2(4)(g) DSA, Art. 1(3) DGA y art. 1(5) del Reglamento de Datos.

[104] El Considerando (12) DMA cita que el mismo reglamento «debe aplicarse sin perjuicio de las normas derivadas de otros actos de derecho de la Unión que regulan determinados aspectos de la prestación de servicios incluidos en el ámbito del presente Reglamento, en particular […] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)».

[105] Art. 5 (2) DMA.

[106] EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),* 2021, § 23; EDPS, *Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative,* 2023, § 27.

de forma genérica la importancia de respetar la normativa de protección de datos y la primacía del RGPD[107].

Aunque la primacía del RGPD sea una cuestión de seguridad jurídica para aquellos casos en los que pueda haber conflicto de normas, la misma está sujeta a dos principales controversias. La primera es el grave problema estructural de esta norma de conflicto[108]. Toda la normativa a la que hemos hecho referencia está marcada en cierta medida por el difícil intento de armonizar dos intereses a menudo contrapuestos: la protección de datos y la economía de datos. Regresando a comparaciones que hemos usado anteriormente, se confrontan el filo del riesgo y el filo de la innovación. Esta contraposición se pone de manifiesto, por ejemplo, en el conflicto entre el principio de minimización de datos y el interés en establecer *data pools* de gran tamaño. No en vano, a menudo la doctrina se refiere a la protección de datos como *el elefante en la habitación* (una suerte de invitado indeseado) para la economía de datos[109].

La segunda controversia es el efecto práctico que entraña la continua remisión al RGPD. En el caso de la prohibición del art. 26.3 de la DSA, se podía haber optado por alternativas más amplias e independientes de conceptos ya regulados por el RGPD[110]. Sin embargo, la prohibición se construye sobre dos conceptos definidos por el RGPD: la elaboración de perfiles y los datos personales sensibles. Si bien el concepto de publicidad basada en la elaboración de perfiles puede plantear menos inconvenientes, el concepto de datos sensibles es un concepto que, desde sus inicios, ha estado sujeto a grandes controversias. La complejidad presente en la regulación de los datos sensibles es tal que se plantea como necesario realizar un análisis más detallado con un doble objeto: *a)* exponer la gran dependencia de la publicidad basada en perfiles sobre la normativa de protección de datos; y *b)* evidenciar cómo la remisión al concepto de datos sensibles supone arrastrar todas las deficiencias que planteaba su regulación.

Dado que el primer gran problema que plantea la definición es la delimitación de la noción de datos personales sensibles, dedicaremos el siguiente capítulo a su análisis.

---

[107] Así, por ejemplo, el considerando (41) señala que el hecho de que un sistema de IA sea considerado de alto riesgo no debe interpretarse como indicador de que su uso sea legal con arreglo al derecho de la Unión relativo a la protección de los datos personales.

[108] Ebers, M. y Sein, K., «Data-driven Technologies…», *op. cit.,* pp. 16-23.

[109] Wendehorst, C. «Of elephants in the room…, *op. cit.*

[110] Se pudo haber optado, por ejemplo, por prohibir la publicidad basada en datos reveladores de vulnerabilidades del usuario, opción que exploraremos en secciones posteriores de este trabajo.

CAPÍTULO II

LA NOCIÓN DE DATOS SENSIBLES Y SU CONCEPTUALIZACIÓN EN EL RGPD. NATURALEZA DE LOS DATOS INFERIDOS Y LOS *PROXIES*, Y DATOS NO INCLUIDOS EN LA LISTA DE DATOS SENSIBLES

I. EL CONCEPTO DE DATOS PERSONALES Y SU TRATAMIENTO

Tanto el ordenamiento jurídico español[1] como el comunitario[2] reconocen como derechos fundamentales la protección de los derechos que las personas físicas tienen respecto al tratamiento que se haga de sus datos personales.

La protección de los datos personales también es un factor esencial en el ámbito de la publicidad. Anteriormente, hemos expuesto cómo el ámbito de aplicación de la prohibición del DSA se circunscribe exclusivamente a la publicidad basada en perfiles desarrollada a partir del tratamiento de datos personales sensibles. Para la adecuada comprensión de la norma, hemos de detenernos previamente a analizar los contornos de dos conceptos clave: los de *tratamiento* y *datos personales*, ya que ambos son la base de la publicidad basada en perfiles.

---

[1] *Vid.* Art. 18.4 CE.

[2] *Vid.* Art. 8.1. de la Carta de los Derechos Fundamentales de la Unión Europea y 16.1 TFUE.

El concepto de tratamiento plantea una menor problemática práctica de cara a la protección de los usuarios, dado su carácter abierto. Así, conforme al RGPD, el tratamiento comprende cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no[3]. En otras palabras, podría afirmarse que toda práctica sobre datos personales es considerada tratamiento, por lo que, por ejemplo, el análisis algorítmico de datos personales para construir perfiles y remitir a los destinatarios una publicidad u otra constituiría, indudablemente, una forma de tratamiento.

En cambio, la definición de los datos personales plantea mayor problemática. Durante años, los intentos de ofrecer una definición exacta de este término han ocupado el puesto central en el debate sobre la normativa europea de protección de datos. Aunque el RGPD ha aportado algo de luz, la discusión se mantiene viva a día de hoy. Si bien su definición puede parecer arbitraria, no lo es en absoluto, puesto que la calificación de los datos como «personales» desencadena el sometimiento a numerosas obligaciones, incluyendo las impuestas por la DSA y la propia normativa de protección de datos[4].

De acuerdo con la definición del RGPD, son datos personales cualquier información relacionada con una persona física identificada o identificable (sujeto de datos). Se considera persona física identificable aquella que puede ser identificada, directa o indirectamente[5]. Por tanto, la identificación —referida tanto a la posibilidad de ser identificado (identificabilidad) como al hecho de ser identificado (identificación efectiva)—, es el criterio delimitador utilizado por la normativa de protección de datos. En aplicación de este criterio distinguiremos los datos personales —relativos a una persona física identificada o identificable—, de los no personales[6].

Poder identificar claramente si estamos ante datos personales o no resulta crítico para la seguridad jurídica de las empresas. Si procesan datos personales, tendrán que cumplir con la normativa de protección de datos, so pena de enfrentarse a multas administrativas que pueden

---

[3] *Vid.* Art. 4.2) RGPD. El artículo establece una lista abierta de prácticas que son consideradas tratamiento, 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».

[4] Purtova, N. «From Knowing by Name to Personalisation: Meaning of Identification Under the GDPR», *SSRN Electronic Journal*, 2021, p. 28.

[5] *Vid.* Art. 2.1 RGPD.

[6] Kindt, E., «Por qué la investigación puede ya no ser la misma: sobre el alcance territorial de la propuesta de Reglamento de Protección de Datos», *Documento de Trabajo 26/2016 del CiTiP*, pp. 13-29.

alcanzar los veinte millones de euros o un 4 por ciento del volumen de negocios total global durante el ejercicio económico anterior[7][8].

A este respecto, el GTA-29 ofreció una indicación para discernir lo que se ha de entender por persona identificada. En términos generales, una persona física puede considerarse identificada cuando, dentro de un grupo de personas, se le distingue de todos los demás miembros del grupo[9], a partir de los rasgos o características que de ella se predican. Es importante subrayar que, de acuerdo con el Grupo de Trabajo y un enfoque literal del RGPD[10], la identificación de un sujeto de datos incluye no solo la identificación por su nombre, sino también otros modos de «acercarse a un individuo de carne y hueso»[11].

Conforme al RGPD, un factor esencial para que los datos sean calificados como personales es que los mismos no estén anonimizados. Aquí entran en juego dos conceptos clave: la seudoanonimización y la anonimización. El RGPD define la seudoanonimización como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable[12]. Los considerandos del RGPD aclaran la diferencia entre ambos términos: los datos sujetos a seudoanonimización son datos relativos a una persona identificable, por lo que están sujetos al Reglamento; mientras que los datos anonimizados son datos referidos a una persona que no puede ser identificada, por lo que quedan fuera de su ámbito de aplicación[13].

Un factor crucial para comprender el alcance exacto del concepto de datos personales es la diferencia entre anonimización y seudoanonimización. La diferencia radica en cuánto esfuerzo tiene que emplear quien accede a los datos para establecer un vínculo entre los datos

---

[7] Art. 83.5 RGPD.

[8] Este 4 por ciento, si bien puede pasar desapercibido, ha generado en la práctica sanciones colosales, siendo la mayor hasta la fecha de 1,2 billones de euros, impuesta a Meta por la Autoridad Irlandesa de Protección de Datos por transferencias de datos personales fuera de la UE. *Vid. Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR).*

[9] Grupo del Artículo 29, *Dictamen sobre el concepto de datos personales*, 2007.

[10] Según el art. 4.1. RGPD, datos personales significa «cualquier información relacionada con una persona física identificada o identificable (sujeto de datos); una persona física identificable es aquella que puede ser identificada, directa o indirectamente*, en particular* por referencia a un identificador *como* un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física» (las cursivas son nuestras).

[11] Grupo del Artículo 29, *Dictamen sobre el concepto…, op. cit.*

[12] *Vid.* art. 4.5) RGPD.

[13] *Vid.* Considerando 29 RGPD.

de los que se dispone y la persona física a la que van referidos o, en otras palabras, qué esfuerzos se requieren para identificar al titular de los datos en cuestión[14]. En este punto se pueden distinguir dos enfoques diferentes.

El primero es un enfoque absoluto, según el cual, si cualquiera en el mundo es capaz de descifrar o decodificar los datos personales cifrados, estaremos ante datos no anonimizados y, por tanto, resultará de aplicación el RGPD[15]. Así, los datos cifrados serán siempre datos personales, porque alguien —al menos el titular de la clave de cifrado o cualquier otra persona con el tiempo, los recursos económicos y la potencia informática suficientes— siempre podrá descodificar los datos, ya que ningún sistema de cifrado es —en abstracto y en teoría— completamente seguro[16].

El segundo enfoque tiene alcance relativo. Según este, solo se tienen en cuenta las posibilidades reales de combinar datos para identificar a un individuo y no los riesgos de identificación altamente teóricos[17]. En consecuencia, la legislación de protección de datos solo es aplicable a los problemas de cifrado si el controlador de datos puede descifrar un determinado conjunto de datos o, al menos, tiene posibilidades razonables de obtener la clave de descifrado. Este enfoque relativo comienza a perfilarse como el preferido por la jurisprudencia de distintos tribunales y órganos administrativos[18].

¿Cuál es el enfoque del RGPD? Según el Reglamento, para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios (como la señalización) que razonablemente puedan utilizarse para identificar directa o indirectamente a la persona física, ya sea por parte del responsable del tratamiento o de cualquier otra

---

[14] Purtova, N. «From Knowing by Name…», *op. cit.*

[15] *Ibid.*

[16] Splinder, G. y Schmechel, P., «Datos personales y cifrado en el Reglamento General Europeo de Protección de Datos», *JIPITEC – Revista de Derecho de la Propiedad Intelectual, Tecnologías de la Información y Comercio Electrónico*, 7, 2016, pp. 162.

[17] *Ibid.*, pp. 174.

[18] Tribunal Superior de Inglaterra y Gales (Tribunal Administrativo), [2011] EWHC 1430 (Admin), Caso No. CO/12544/2009, considerando 51 y ss.;Tribunal Superior (Sala de lo Contencioso-Administrativo de Apelaciones), [2011] UKUT 153 (AAC), número de recurso: GI/150/2011, GI/151/2011, GI/152/2011, considerando 128; House of Lords, [2008] UKHL 47, considerando 27;Sentencia del Tribunal de Apelación de París, de 15 de mayo de 2007 – Henri S. c. SCPP;Sentencia del Tribunal de Primera Instancia de Múnich, de 30 de septiembre de 2008-133 C 5677/08– 133 C 5677/08, considerando 26;Sentencia del Tribunal de Distrito de Wuppertal, de 19 de octubre de 2010-25 Qs 10 Js 1977/08-177/10;Sentencia del Tribunal de Primera Instancia de Berlín, de 31 de enero de 2013-57 S 87/08– 57 S 87/08; diferentes puntos de vista: The Stockholm Lænsrætt, referencia núm. 593-2005, fecha de publicación 8 de junio de 2005; Tribunal de Primera Instancia de Berlín-Mitte, sentencia de 27 de marzo de 2007-5 C 314/06, considerando 20; Tribunal de lo Contencioso-Administrativo de Wiesbaden, sentencia de 27 de febrero de 2009-6 K 1045/08.WI, considerandos 52 y ss.

persona[19]. Aquí hay dos factores fundamentales y contradictorios: la alusión a «razonablemente» y la alusión a «cualquier otra persona».

La expresión «razonablemente» sugiere una proximidad al enfoque relativo, que tiene en cuenta los esfuerzos que el responsable del tratamiento ha de realizar para identificar (o no identificar) al interesado. Por contraposición, la alusión a «cualquier otra persona» se acerca más a un enfoque absoluto, según el cual, si al menos una persona en el mundo es capaz de descifrar o decodificar los datos personales cifrados, el RGPD resultará de aplicación[20].

Otro aspecto a tener en cuenta a la hora de plantear la identificación es el contexto. En un momento determinado, los datos personales pueden ser anónimos, perdiendo, por tanto, su carácter de datos personales y quedando fuera del ámbito de aplicación del RGPD. Algún tiempo después, se puede poner a disposición pública más información, lo que permite la combinación de diferentes datos para identificar a los interesados cubiertos por una anonimización inicial[21].

En consecuencia, ningún dato personal puede ser completamente anónimo de forma perpetua y absoluta. Desde un enfoque relativo, para que los datos queden anonimizados, bastaría con aplicar un proceso razonablemente complejo de cifrado, mediante el cual, a la hora de evaluar si los datos entran dentro del ámbito de aplicación del RGPD, solo se tengan en cuenta las posibilidades reales de combinar datos para identificar a una persona. A nuestro entender —siguiendo a una gran mayoría de autores—, el enfoque absoluto constituye una carga excesivamente pesada para el responsable del tratamiento, ya que muchos estudios científicos reflejan que ningún sistema de cifrado puede ser completamente seguro[22].

Por este motivo, el TGUE se ha apartado de la postura absoluta, la cual venía afirmando que, si cualquier persona en el mundo puede identificar al interesado, los datos no son anónimos[23]. Conforme al TGUE, los datos trasmitidos a un tercero pueden considerarse anónimos cuando el destinatario no disponga, razonablemente, de los medios para volver a identificar al interesado. El hecho de que el transmisor de los datos disponga de medios para identificar a los interesados no significa que los datos comunicados sean datos personales para el destinatario.

---

[19] *Vid.* Considerando (26) RGPD.

[20] Splinder, G. y Schmechel, P. «Datos personales y cifrado…», *op. cit.*

[21] Purtova, N. «From Knowing by Name…», *op. cit.*

[22] *Ibid.*

[23] Sentencia del Tribunal General de la Unión Europea, de 26 de abril de 2023, asunto T-557/20, *Junta Única de Resolución y Supervisor Europeo de Protección de Datos* (ECLI:EU:T:2023:219).

En el caso en cuestión que fue llevado ante el Tribunal, el código alfanumérico que figuraba en cada respuesta no permitía al destinatario revelar directamente la identidad de la persona física que había cumplimentado el formulario, por lo que el Alto Tribunal Europeo consideró que los datos tenían carácter anónimo para el destinatario. Por tanto, los datos se considerarán anónimos y no tendrán el carácter de personales si el destinatario no dispone de medios razonables para identificar a los interesados.

¿Qué consecuencias tiene la adopción de este enfoque relativo para la publicidad basada en perfiles? Por lo general, la anonimización tiene un margen de aplicación bastante limitado en el ámbito publicitario, ya que la publicidad basada en perfiles implica, necesariamente, el tratamiento de un mínimo de datos personales, al basarse en la identificación del usuario, y la segmentación del público objetivo general al cual se puede dirigir la actividad publicitaria. Aunque el perfil aplicado sea un perfil grupal construido con base a unas características predeterminadas, una vez que estas características se apliquen al destinatario de la publicidad, pasarán a ser datos personales, ya que se refieren a un sujeto identificado o identificable. En consecuencia, la aplicación de dicho perfil no sería sino otra forma más de tratamiento de datos personales.

Aunque el algoritmo que construye el perfil no tuviese acceso al nombre del usuario, sino a otros identificadores como la dirección IP o las cookies, seguiría tratando datos personales, puesto que los mismos transcienden más allá del nombre, al referirse a cualquier información que haga que el usuario pueda ser identificable[24]. En conclusión, la publicidad personalizada necesita alimentarse de cantidades masivas de datos personales del usuario para resultar efectiva, por lo que, al tratar datos personales, caerá imperativamente dentro del ámbito de aplicación de la normativa de protección de datos.

II. ¿SON LOS DATOS INFERIDOS DATOS PERSONALES?

El tratamiento de datos personales está presente desde nuestra más tierna infancia hasta el momento en el que un médico certifica nuestra muerte (e incluso, si somos precisos, después)[25]. Cuando nacemos, datos como nuestro nombre, peso y hora de nacimiento quedan

[24] *Vid.* Considerando 30 RGPD.

[25] Por ejemplo, en España, la LOPD reconoce en su art. 3.1 que las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

registrados en nuestra historia clínica[26]. Lo mismo sucede con la inscripción de nacimiento en el Registro Civil en España, que se refleja a través de un asiento registral con la fecha, hora y lugar de nacimiento, identidad, sexo y, en su caso, filiación[27]. Cuando somos inscritos en nuestra primera guardería o colegio, este guarda un registro con nuestros datos y los datos de contacto de nuestros familiares, por si surge una emergencia. Cuando accedemos a nuestro primer empleo sucede lo mismo, la empresa recabará información como nuestro número de teléfono, IBAN, DNI y número de la Seguridad Social. Si realizamos una tarea tan simple como pedir comida a domicilio, la empresa de reparto necesitará una dirección en la que entregar el pedido.

Nadie en la doctrina pone en entredicho que todas estas actividades constituyen un tratamiento de datos personales. A pesar de que la normativa sobre protección de datos personales experimenta una evolución a lo largo del tiempo, el procesamiento de datos personales sobre diversas vicisitudes de nuestra existencia es una realidad constante en las relaciones sociales y humanas. Precisamente, este carácter constante ha hecho que perdamos consciencia de la importancia que puede tener el tratamiento de datos personales para nuestra privacidad. Vivimos en la paradoja de no querer tirar papeles con nuestro nombre a la basura, mientras que, al mismo tiempo, accedemos a una página web aceptando todas las cookies, funcionales y no funcionales.

El ciudadano desconoce con carácter general el uso que se hace de sus datos. Netflix nos recomienda series y películas que tal vez nos puedan gustar, y la precisión de las recomendaciones es sorprendentemente alta. Nos desplazamos por la sección «explora» de Instagram, y todos los contenidos nos resultan interesantes. YouTube nos recomienda vídeos, y resulta que casan excelentemente bien con nuestros gustos. Los contenidos sugeridos por diversas plataformas parecen encajar con las ideas que teníamos sobre ciertos partidos políticos, o sobre algunos diputados en particular. Las noticias que recibimos confirman lo que ya sospechábamos sobre la nueva reforma que se está debatiendo en el Congreso. En la palma de nuestra mano (o de nuestro *smartphone*) descansan todas nuestras ideas preconcebidas, gustos, prejuicios, miedos, tendencias… tanto las que sabemos que tenemos, como las que no, pero que inconscientemente vienen vinculadas a nuestra personalidad.

Todos estos fenómenos son posibles gracias al tratamiento automatizado de nuestros datos personales. Si queremos ser más precisos, en muchos de estos casos hablaríamos no de datos personales en general, sino de *proxies* y datos inferidos, recabados con el objeto de microsegmentar a la población. La pregunta práctica que aquí plan-

[26] Art. 15.3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

[27] Art. 4 de la Ley 20/2011, de 21 de julio, del Registro Civil.

teamos es si los datos inferidos son datos personales y si, por ende, gozan de la protección que se le otorga jurídicamente a estos últimos. En este último caso, resultará necesario que concurra una base legal para su procesamiento, y su uso se someterá a todos los principios y reglas aplicables bajo la normativa de protección de datos.

Para intentar responder a esta cuestión, el primer paso es plantear qué debemos entender por datos inferidos, también denominados inferencias o datos «nuevos»[28]. Los datos inferidos son aquellos datos obtenidos a partir del tratamiento de un conjunto amplio de datos o *proxies*, analizados mediante tecnologías como el *Big data* y la Inteligencia Artificial.[29] A través de los datos inferidos, el algoritmo publicitario puede adaptar qué publicidad recibe cada destinatario concreto, lo que se conoce como publicidad basada en perfiles individuales. Estos perfiles pueden ser diseñados específicamente para cada usuario en concreto, o pueden ser previamente elaborados y asignados a un destinatario que presente afinidad con un grupo preconfigurado. En este último caso, cualquier tercero interesado —como un anunciante— puede definir distintos grupos estableciendo, por ejemplo, que pertenecen a un grupo aquellas personas que tienen el mismo tipo de automóvil, que compran un tipo de comida, que comparten el mismo nivel adquisitivo, que seleccionan el mismo contenido *online*, que viven en el mismo barrio, que sufren la misma infección, etc. Estos grupos, definidos *ad hoc*, no cuentan con un listado de miembros, pues sus contornos se desarrollan sobre perfiles abstractos, y sus integrantes posteriores no son siempre conscientes de su inclusión o pertenencia a los mismos[30].

La construcción de estos perfiles abstractos se realiza mediante un sistema de procesamiento informatizado, normalmente aplicando Inteligencia Artificial, que sigue el siguiente proceso secuencial: 1) recolección de datos, 2) construcción del modelo y 3) implementación del modelo[31]. En el caso de los datos inferidos, el sistema de IA recaba en la primera fase una serie de *proxies* o datos de toda clase de sujetos (como los antes descritos). En la segunda fase analiza dichos datos personales, infiere otros nuevos y construye los perfiles abstractos en base tanto a los datos recolectados como a los inferidos. Por último,

---

[28] Wachter, S. «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbian Business Law Review*, 2, 2019, pp. 436-449.

[29] *Proxy* es un término utilizado por programadores para referirse a «indicadores» del objetivo que se pretende conseguir, pero que el ordenador no puede discernir por sí mismo. Estos *proxies* sirven como una aproximación a cierta información a la que no se tiene acceso directo o a la que el programador prefiere no tener acceso directo. AEPD, «oT (I): Qué es IoT y cuáles son sus riesgos», 2020.

[30] AEPD, «Privacidad de grupo», 2020.

[31] Castillo Parrilla, J.A. «Privacidad de grupo…», *op. cit.*

en la tercera fase, casa estos perfiles abstractos con cada destinatario en particular.

Pongamos un ejemplo sencillo. En la primera fase, el sistema de IA es alimentado con toda clase de datos personales derivados de diversas fuentes, como cookies analíticas. En la segunda fase, el sistema de IA analiza todos estos datos e infiere que los destinatarios que presentan una serie de características son tendentes a presentar también otras. Estas características o datos iniciales pueden ser, por ejemplo, que Google Maps revele datos de localización sobre una visita continuada a estancos, a bares de copas y a restaurantes de comida rápida, y que, por su lado, el historial de reloj inteligente muestre pulsaciones elevadas frecuentes, escasas horas de sueño profundo y ningún dato sobre deportes realizados. El sistema de IA, con base a esta información, infiere nuevos datos (datos inferidos) como el elevado riesgo de cáncer, infarto o ictus cerebral, conformando un perfil abstracto con base a estos datos. En la tercera fase identifica a algunos sujetos como pertenecientes a este perfil y los incluye en algunos grupos —receptores de anuncios sobre bebidas alcohólicas— y los excluye de otros —receptores de anuncios sobre determinadas ofertas de seguros de vida y de créditos bancarios—.

Los datos inferidos serán datos personales si conforman una información capaz de identificar, directa o indirectamente, a una persona física[32]. Si retornamos a las etapas del proceso anterior, los datos inferidos surgen en la segunda fase del proceso realizado por la IA. En esta segunda fase —construcción del modelo—, los datos inferidos no son capaces de identificar a una persona física, ya que sirven meramente para la construcción de perfiles abstractos, sin tener una aplicación práctica. Ahora bien, en la tercera fase —aplicación del modelo— sí que cobran la naturaleza de datos personales, ya que los perfiles abstractos, conformados por datos inferidos y demás datos, se aplican a una persona concreta. Señalan acertadamente algunos autores que, aunque estos conocimientos nuevos sean más o menos precisos en términos de probabilidad, se está realizando una actividad de tratamiento como cualquier otra, al establecer una relación de semejanza suficientemente relevante entre el perfil abstracto y la persona, al afirmar que dicho perfil funciona para una persona concreta y, previsiblemente, se comportará del mismo modo que los demás componentes de ese grupo[33].

Este planteamiento queda confirmado de una forma más detallada si acudimos al modelo de tres pasos propuesto por el Grupo de Trabajo del Artículo 29 para determinar cuándo los datos son datos persona-

[32] *Vid.* Art. 2.1 GDPR.

[33] Castillo Parrilla, J. A. «Privacidad de grupo…», *op. cit.*

les[34]. Este modelo permite transformar datos no personales en datos personales al relacionarlos con una persona identificable, ya sea directa o indirectamente, a través de un examen basado en tres criterios. Si se cumple cualquiera de estos pasos o criterios, los datos serían datos personales.

El primer paso consiste en examinar el contenido del tratamiento de los datos. Si el contenido del dato permite describir directamente a una persona, serán considerados datos personales. El segundo paso se refiere al propósito del tratamiento. Si los datos son tratados para evaluar, tratar de determinada manera o influenciar a una persona, tendrán la naturaleza de datos personales. El tercer paso es el resultado de su tratamiento. Este paso es particularmente importante para justificar la naturaleza personal de las inferencias. Según el Grupo de Trabajo, bajo este paso, es suficiente con que los datos tengan un impacto posible en los derechos e intereses de una persona para que sean considerados datos personales, sin que sea necesario que concurran los pasos del contenido o del propósito[35]. En otras palabras, si los datos inferidos tienen el potencial de impactar en los derechos e intereses de una persona, serán considerados datos personales.

En el caso de los datos inferidos por algoritmos publicitarios será bastante usual que se cumpla este modelo en cualquiera de sus pasos, ya que los datos inferidos se usan para describir a un sujeto en particular (paso del «contenido»), con el objetivo de influenciar su comportamiento de cara a un anuncio (paso del «propósito»), y este uso tiene como consecuencia la adaptación o limitación de las ofertas que recibe la persona (paso del «resultado»)[36].

El carácter personal de los datos inferidos aplicados a perfiles de personas concretas quedó confirmado igualmente por el GT29 en su guía sobre portabilidad de datos personales, en la cual distingue dos categorías de datos personales en función de su origen[37]. La primera categoría son los datos aportados por el propio sujeto de datos, ya sea de modo activo y consciente (por ejemplo, al aportar su dirección de correo electrónico), ya sea mediante el uso de un dispositivo o servicio (como el historial de búsqueda o la localización). La segunda categoría son los datos inferidos o derivados, que comprenden aquellos datos creados por el responsable del tratamiento a partir de los datos

---

[34] Grupo de Trabajo del Artículo 29 Sobre Protección de Datos, «Dictamen 4/2007 sobre el concepto de datos personales», 2007, pp. 8-12.

[35] *Ibid.*

[36] Bajo el apartado destinado a los datos sensibles, ejemplificaremos algunos casos en los que los datos inferidos tienen peligrosos resultados sobre derechos fundamentales de las personas.

[37] Article 29 Data Protection Working Party, «Guidelines on the right to data portability», 2016, pp. 9-17.

aportados por el sujeto de datos, incluyendo los datos creados por procesos algorítmicos. Conforme a la guía del Grupo de Trabajo, algunos ejemplos de datos inferidos son los datos derivados de una valoración sobre el estado de salud de un sujeto, o los datos derivados de un perfil creado para establecer una puntuación de crédito, para cumplir con reglas sobre la prevención del blanqueo de capitales o, incluso, para completar un proceso de personalización y recomendación. Finalmente, el Grupo de Trabajo también se refiere a los datos inferidos en su guía sobre construcción de perfiles y toma automatizada de decisiones, al señalar que la construcción de perfiles se basa en la creación de datos derivados o inferidos sobre individuos, es decir, datos personales *nuevos* que no han sido aportados por el sujeto de datos[38].

Todo este planteamiento quedó confirmado, si bien de forma más escueta, por el TJUE, en el caso *Vyriausioji tarnybinės etikos komisija*[39]. La Gran Sala del Alto Tribunal optó por una interpretación amplia del concepto de datos personales sensibles, afirmando que el mismo engloba no solo los datos intrínsecamente sensibles, sino también aquellos datos personales que «desvelen indirectamente, mediante un ejercicio intelectual de deducción o de cruce de datos, informaciones de esta naturaleza».

Ahora bien, es cierto que los datos inferidos pueden tener un margen de imprecisión como, por ejemplo, que el dispositivo sea utilizado por varias personas de un núcleo familiar[40], por lo que el perfil aplicado no identificaría a una sola persona física, conforme requiere el RGPD. Sin embargo, este problema también se presenta con los datos no inferidos y aun así se tiende a reconocer que los datos personales continúan siéndolo pese a que exista un margen de error sobre el sujeto al que potencialmente pueden identificar.

Igualmente, este margen de imprecisión comprende que los datos inferidos puedan no ser acertados, es decir, que se asuma que el individuo presente una característica que en realidad no posee[41]. Sin embargo, en la práctica, no es necesario que estos datos inferidos sean

---

[38] Article 29 Data Protection Working Party, *Guidelines on Automated individual…*, *op. cit.,* p.8.

[39] STJUE *Viriausioji tarnybinės etikos komisija*, de 1 de agosto de 2022, asunto C-184/20, ECLI:EU:C:2022:601.

[40] Esta problemática es reconocida por Google, al tratar los datos demográficos inferidos en la sección «glosario». *Vid. https://support.google.com/surveys/answer/6218151?hl=es.*

[41] En LinkedIn se hizo viral un post en el que se advertía de la importancia de segmentar correctamente. El ejemplo aportado era el siguiente: en un lado, se presentaba al rey Carlos III de Inglaterra, en el otro, al cantante de heavy metal Ozzy Osbourne. Ambos eran descritos bajo las mismas características: hombre, nacido en 1948, educado en Reino Unido, casado dos veces, vive en un castillo, rico y famoso. Esta publicación revela el riesgo de que el algoritmo elabore los mismos datos inferidos sobre ambas personas y que, sin embargo, las inferencias sean totalmente erróneas, ya que es presumible que los intereses de ambos sujetos varíen notablemente.

certeros. Como señala el GT29, la intención del legislador es establecer una definición amplia de datos personales, incluyendo información relativa a un individuo identificado o identificable, sin que esta información tenga que ser necesariamente cierta o probada[42].

Por último, quedan dos cuestiones o problemáticas por plantear. La primera, si asumimos que los datos inferidos son datos personales por las razones anteriormente expuestas, éstos, como cualquier dato personal, se deberán someter a la ulterior clasificación encajando en una de las dos opciones posibles: la de datos personales *generales*, y la de categorías especiales de datos personales (también denominados *datos sensibles*). El hecho de que los datos se califiquen como de uno u otro tipo despliega singulares consecuencias jurídicas, ya que los requisitos para su tratamiento variarán notablemente bajo el RGPD y la DSA.

La segunda cuestión viene referida a la trazabilidad del proceso algorítmico. En concreto nos referimos a qué sucede cuando el proceso algorítmico no muestra ni añade nuevos datos (datos inferidos), sino que es la mera combinación de diferentes datos o *proxies* de naturaleza no sensible de la que resulta un trato discriminatorio o adverso, y este trato es consecuencia de una conclusión que, a ojos humanos, presenta *naturaleza sensible*, pero en ningún momento del proceso algorítmico es trazable. Trataremos ambas problemáticas en el siguiente apartado.

III. CONCEPTO, RAZÓN DE SER Y TIPOLOGÍA DE DATOS PERSONALES SENSIBLES. EL PROBLEMA DE LOS PROXIES Y LOS DATOS SENSIBLES INFERIDOS

1. Concepto, antecedentes y razón de ser de los datos sensibles

Una de las principales preocupaciones en torno a la regulación de la publicidad personalizada radica en cómo paliar la manipulación de las vulnerabilidades del destinatario, en la cual el manejo de datos sensibles desempeña un papel protagonista. Los datos sensibles, denominados en el RGPD *categorías especiales de datos*, presentan una regulación específica y reforzada, tanto en lo relativo a su tratamiento como en cuanto a la toma de decisiones automatizadas basadas en ellos[43].

---

[42] STJUE *Vyriausioji tarnybinės etikos komisija*, de 1 de agosto de 2022, asunto C-184/20, ECLI:EU:C:2022:601.

[43] *Vid.* Asunto C-465/ 00, *Rechnungshof*, para. 75, en el que se afirma que «para demostrar la existencia de tal injerencia, es indiferente que la información comunicada sea de carácter sensible o que las personas afectadas hayan sido molestadas de alguna manera».

Bajo la categoría de datos sensibles, el RGPD se refiere a todos aquellos datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física[44]. En un principio, bajo la anterior —y ya derogada— Directiva de Datos Personales, ni los datos genéticos ni los datos biométricos aparecían considerados como categorías especiales de datos, pero fueron posteriormente incluidos en el RGPD[45].

La lista de datos personales sensibles que ofrece el RGPD es una lista exhaustiva o cerrada, es decir, los Estados Miembros no pueden añadir nuevas categorías a la lista, si bien la norma les deja un amplio margen de maniobra para especificar las normas aplicables al tratamiento de datos sensibles[46]. De todas las categorías de datos sensibles, solo tres son definidas por el propio RGPD, a saber, los datos genéticos[47], los datos biométricos[48] y los datos relativos a la salud[49]. Ahora bien, la falta de una definición específica de las otras cinco categorías de datos sensibles no se traduce en una absoluta incertidumbre sobre las mismas[50]. Bajo diferentes métodos interpretativos, procederemos seguidamente a caracterizar cada una de las categorías de datos sensibles.

Para entender por qué es necesaria una regulación específica de los datos sensibles, es necesario que atendamos no solo al RGPD, sino también, aunque sea brevemente, a su origen y a otros instrumentos internacionales en los que se exponen razones comunes para la protección *sui generis* de los datos sensibles.

Fue el Convenio nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, y su Protocolo Adicional de 8 de noviembre de 2001, el que introdujo la categoría de datos sensibles

---

[44] *Vid.* Art. 9.1. RGPD.

[45] Voigt, P. y Von Dem Bussche, A. *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, 2017, pp. 92-116.

[46] *Vid.* Considerando 51 RGPD. La consideración de la lista del art 9.2 del RGPD como *numerus clausus* se desprende no solo de la redacción del precepto, sino también del considerando (51). En la consulta número 054388/2019, la AEPD señaló que «las categorías especiales de datos se han de considerar numerus clausus, pues conforman un régimen especial de protección que supone una excepción que limita y circunscribe a unos supuestos específicos las posibilidades de tratamiento, por lo que la interpretación que se realice debe ser restrictiva».

[47] *Vid.* Art. 4.13 RGDP.

[48] *Vid.* Art. 4.14 RGPD.

[49] *Vid.* Art. 4.15 RGPD.

[50] Ludmila, G. y Kuner, C., «Article 9 Processing of special categories of personal data» in Kuner, C. *et al., The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, 2020.

o datos especialmente protegidos. La legislación internacional ha ido contemplando para estos datos previsiones específicas, considerándolos elementos de la personalidad del individuo, vinculados a su dignidad personal[51]. El Convenio fue ratificado por España en 1982 y se refería a lo que hoy conocemos como datos sensibles o categorías especiales de datos personales bajo la terminología de «categorías particulares de datos». Así, señalaba que los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La *raison d'être* de este tratamiento especial queda más desarrollada en el Informe Explicativo del Convenio, en el cual se mencionan no solo los riesgos de discriminación, sino también otros efectos adversos como los daños a la dignidad, a la integridad física o a la presunción de inocencia.

Posteriormente, las Directrices para la regulación de los archivos de datos personales informatizados adoptadas por las Naciones Unidas en 1990 ya se referían a los *datos sensibles*, si bien no bajo dicha denominación explícita, señalando que «no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato».

A nivel de la UE, la Directiva de Protección de Datos (antecesora del RGPD) (en adelante, «DPD») ya incorporaba las categorías especiales de datos personales, si bien todavía no mencionaba ni los datos genéticos ni los biométricos[52]. A pesar de que la Directiva destinaba un artículo específico a la regulación de datos sensibles[53], los considerandos de la misma no llegaban a justificar el tratamiento particular de los mismos, sino que justificaban la necesidad de protección de los datos personales en general, remitiéndose al deber de garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el CEDH, así como en los principios generales del derecho comunitario[54].

---

[51] Gómez Sánchez, Y. «Categorías especiales de datos personales: los datos de origen étnico o racial, los datos genéticos, los datos biométricos, los datos relativos a la salud, los datos relativos a la vida sexual y a la orientación sexual (comentario al art. 9.1. RGPD)», en Troncoso Reigada, A. *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales,* Tomo I, Aranzadi, 2021, pp.1041-1042.

[52] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

[53] *Vid.* Art. 8 DPD.

[54] *Vid.* Considerando 10 DPD.

Las razones fundamentales para una regulación *sui generis* de los datos sensibles sí serían posteriormente desarrolladas por los considerandos del RGPD. La parte expositiva de la norma señala que merecen una protección especial aquellos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para estos últimos[55]. Igualmente, al tratar el derecho del sujeto de datos a no estar sujeto a decisiones individuales automatizadas, los considerandos se refieren de forma particular a los datos sensibles. Así, señalan que el responsable del tratamiento debe tomar medidas para impedir, entre otras cosas, *efectos discriminatorios* por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, clarificando que las decisiones automatizadas y la elaboración de perfiles sobre la base de datos sensibles únicamente deben permitirse *en condiciones específicas*[56].

Por otro lado, en la propuesta de Reglamento sobre privacidad electrónica también se exponen las razones por las que los datos sensibles tienen un carácter especial digno de protección adicional[57]. La propuesta no usa el término «datos sensibles» ni «categorías especiales de datos personales», sino que se refiere a *información muy delicada*. Conforme a los considerandos de la propuesta, la divulgación de esta información muy delicada «podría causar daños personales y sociales, pérdidas económicas o situaciones embarazosas»[58]. La diferencia más notable respecto al resto de normas internacionales señaladas es que, bajo la propuesta, no se llega a mencionar directamente el riesgo de discriminación, sino que se basa en una justificación más genérica[59].

En consecuencia, cabe concluir que la *raison d'être* de establecer una regulación específica sobre los datos sensibles no es otra que la protección de los individuos frente a posibles efectos adversos derivados del uso (o abuso) de tales datos. Conforme a los textos internacionales citados, tales efectos adversos incluyen, en términos generales, poner en riesgo los derechos y libertades de los individuos, lo que incluye la discriminación[60]; pero también —de forma más particular—

---

[55] *Vid.* Considerando 51 RGPD.

[56] *Vid.* Considerando 51 RGPD.

[57] Propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/C.

[58] *Vid.* Considerando 2 de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas.

[59] Malgieri, G. y Quinn, P. «The Difficulty of Defining Sensitive Data. The concept of sensitive data in the EU data Protection framework», *German Law Journal*, 2020.

[60] Voigt, P. y Von Dem Bussche, A. *The EU General Data Protection Regulation…, op. cit.,* pp. 92-116.

posibles daños físicos, psíquicos, sociales o económicos[61]. Esta idea se mantendrá a lo largo del presente estudio, en el cual desarrollaremos los posibles daños derivados del tratamiento de datos sensibles para fines de publicidad basada en perfiles.

2. La disyuntiva de la naturaleza de los *proxies* y los datos inferidos

El concepto de datos sensibles es un concepto que no ha sido ajeno a los avances tecnológicos. Gracias al *Big data*, el Internet de las Cosas, el surgimiento de complejos algoritmos y sistemas de IA, en la última década los datos sensibles han sufrido una reformulación práctica que se traduce en una necesidad de actualización jurídica.

Cuando el RGPD entró en vigor, el concepto de datos personales sensibles ya acumulaba ciertos problemas no resueltos derivados de normas anteriores, como la DPD. Uno de ellos era la definición misma del concepto, basada en una aproximación aislada. Conforme a esta definición, acogida por la literalidad del RGPD, el carácter sensible de los datos personales se basa en la naturaleza objetiva de los datos en sí mismos, sin considerar el propósito con el que son tratados[62]. La única excepción en el RGPD a esta definición aislada se encuentra en los datos biométricos. Así, cuando los considerandos y el articulado del RGPD se refieren a la regulación de los datos sensibles, no mencionan el propósito con el que éstos deben ser tratados para merecer tal consideración, a excepción de los datos biométricos. Sobre éstos, el Reglamento exige que sean tratados con el objetivo de «identificar de manera unívoca a una persona física»[63].

Para que los datos en general tengan la consideración de datos personales bajo el RGPD deben referirse a un sujeto identificado o identificable. Pero el requisito de la identificabilidad es un concepto bien distinto al propósito del tratamiento, ya que los fines del tratamiento pueden ser variados e indiferentes a la identificabilidad, como es el caso de la elaboración de estadísticas. En otras palabras, el responsable de datos puede tratar datos personales que se refieran a un sujeto identificable, pero el tratamiento puede no tener como propósito identificar a los sujetos a los que los datos se refieren. En cambio, en el caso de los datos biométricos, el RGPD sí exige que el fin del tratamiento sea la identificación unívoca del sujeto. A nuestro entender y el de muchos autores, la razón de esta divergencia radica en que el legislador comu-

---

[61] Malgieri, G. «Data protection principles and vulnerable data subjects» in Malgieri, G. *Vulnerability and Data Protection Law*, Oxford University Press, 2023, pp. 101-129.

[62] Wachter, S. «A Right to Reasonable Inferences…», *op. cit.*

[63] *Vid.* Art. 9.1 RGPD.

nitario quiso evitar que todas las fotografías y vídeos en los que aparezcan personas físicas caigan bajo la regulación *sui generis* de los datos sensibles[64].

Con la salvedad de los datos biométricos, el RGPD presenta una definición excesivamente constreñida de los datos sensibles. Ya mientras la DPD estaba en vigor, algunos autores señalaban que la definición contextual de los datos sensibles podía fomentar que los responsables de tratamiento llegasen a conclusiones que pudiesen presentar naturaleza sensible[65]. Igualmente, otros autores señalaron que la extrema amplitud del concepto hace imposible una definición real de los datos sensibles, que permita una aproximación que tenga en cuenta el propósito del tratamiento[66].

Sobre la base de esta problemática, surge el dilema de qué sucede cuando los datos personales de entrada (*inputs*) no son claramente datos sensibles, sino que, de forma indirecta o agregada, pueden revelar funcionalmente datos nuevos que sí lo son, como la raza, el estado de salud, las ideas políticas o la orientación sexual (es decir, datos inferidos de naturaleza sensible). Generalmente, los datos inferidos pueden obtenerse a través de *proxies,* como adelantábamos, un término utilizado por programadores para basarse en *indicadores* del objetivo que se pretende conseguir, pero que el ordenador no puede discernir por sí mismo. De este modo, los *proxies* sirven como una aproximación a cierta información a la que no se tiene acceso directo o a la que el programador prefiere no tener acceso directo[67].

Un clásico ejemplo sería el uso de *proxies* para evitar procesar datos relativos a la raza de los individuos —eludiendo las obligaciones derivadas del tratamiento de datos sensibles— procesando en su lugar, por ejemplo, códigos postales —ya que en muchas ciudades vivir en determinados barrios puede ser un *proxy* muy efectivo para inferir orígenes étnicos—[68]. Otro ejemplo a menudo utilizado para referirse al potencial discriminatorio de los *proxies* es la identificación de la orientación sexual del usuario a través del análisis de sus contactos en redes. Así, hay estudios que muestran que el porcentaje de amigos

---

[64] *Vid.* por todos, Malgieri, G. y Quinn, P. «The Difficulty of Defining…», *op. cit.*

[65] Poullet, Y. y Dinant, J. M., «Report on The Application of Data Protection Principles to the Worldwide Telecommunication Networks: Information Self-Determination in The Internet Era: Thoughts on Convention For The Purposes Of The Future Work Of The Consultative Committee», núm. 108, 2004.

[66] McCullagh, K. «Data Sensitivity: Proposals for Resolving the Conundrum», *Journal of International Commercial Law and Technology*, vol. 2, Issue 4, 2007, pp. 190-201.

[67] Huergo Lora, A. «Una aproximación a los algoritmos desde el derecho Administrativo», en Huergo Lora, A. y Díaz González, G. *La regulación de los algoritmos*, Aranzadi, 2020, pp. 23-59.

[68] Calabresi, G. «Ideals, Beliefs, Attitudes, and the Law: Private Law Perspectives on a Public Law Problem», *Syracuse University Press,* 1995, pp. 35-36.

de un usuario en Facebook que se autoidentifiquen como homosexuales en la plataforma está estrechamente relacionado con la orientación sexual del usuario en cuestión[69].

Si relacionamos este uso con el apartado anterior relativo a los datos inferidos, podemos reseñar que, en publicidad, encontramos dos usos distintos de *proxies*.

El primer uso de *proxies* se basa en utilizar o combinar datos originarios para crear datos nuevos inferidos. Estos últimos serán utilizados para construir un perfil abstracto que se aplique posteriormente a un sujeto de datos concreto, produciéndose una actividad de tratamiento como cualquier otra. En apartados anteriores, exponíamos cómo estos datos inferidos presentan la naturaleza de datos personales. Damos aquí por reproducidas las razones mantenidas entonces. Constatada la naturaleza personal de los datos inferidos, planteábamos la cuestión de que, si los datos inferidos son datos personales, deben necesariamente pertenecer bien a la categoría de datos personales genéricos, o bien, a la categoría de datos personales sensibles.

Sin embargo, la respuesta a esta categorización no siempre resulta clara. Mediante el uso de *proxies,* pueden inferirse datos nuevos cuyo carácter sensible sea discutible. En palabras de algunos autores, este fenómeno se plasma en que «una mayor cantidad de datos se traduce probablemente en más datos sensibles»[70]. Así, por ejemplo, pueden utilizarse determinados *proxies* —como datos de localización sobre visitas a estancos— para inferir que el sujeto es fumador. Este nuevo dato es, claramente, un dato que revela hábitos poco saludables del individuo, pero ¿puede ser considerado un dato relativo a la salud, a efectos del RGPD, o nos encontramos meramente ante otro *proxy* que sirve como indicador del estado de salud? Si el dato inferido es considerado inequívocamente un dato sensible, quedaría sujeto a la normativa, por lo que, en principio, este dato inferido no podría utilizarse por servicios de plataforma para presentar publicidad basada en perfiles[71]. Si, en cambio, su calificación como dato personal sensible no es tan clara, se le aplicaría el proceso que analizaremos a continuación.

El segundo uso de *proxies* se basa en combinar distintos *proxies* sin llegar a crear datos nuevos. Siguiendo esta práctica, el algoritmo publicitario recabaría una serie de datos personales de carácter no sensible —*proxies «*no sensibles»— que sirven para tomar decisiones automatizadas basadas en conclusiones que pueden ser de naturaleza

---

[69] Zuiderveen, B. «Discrimination, artificial intelligence and algorithmic decision-making», *Council of Europe, Directorate General of Democracy*, pp. 30-49.

[70] En la versión original inglesa, «more data is likely to mean more sensitive data». *Vid.* Malgieri, G. y Quinn, P. «The Difficulty of Defining…», *op. cit.*

[71] Art. 26.3 DSA.

sensible. Pero estas conclusiones no se trazan ni plasman en nuevos datos en ningún momento del proceso algorítmico, lo que permite escapar de la normativa más severa aplicada a los datos sensibles. Conforme a este uso de *proxies,* nos encontraríamos ante un resultado que es fruto de una toma de decisiones puramente automatizada, en la que los posibles sesgos presentes en los *inputs* dan lugar a *outputs* igualmente sesgados o incluso discriminatorios[72]. Así, por ejemplo, los algoritmos pueden estar sesgados inadvertidamente, favoreciendo a los hombres sobre las mujeres en anuncios sobre trabajos STEM en plataformas como Facebook, Google, Instagram y Twitter, al detectar que la mayoría de los trabajadores en estas ramas son hombres y concluir que, al ser el perfil más contratado por la empresa anteriormente, el perfil masculino es el más adecuado a la oferta[73].

En protección de datos, la problemática que presenta este uso de *proxies* es que los mismos pueden escapar de la protección que otorga el RGPD a los datos sensibles, ya que no revelan directamente este carácter, sino que, analizados en conjunto, muestran el grado de afinidad del sujeto de datos hacia ciertos grupos protegidos[74]. Este grupo protegido — por ejemplo, el colectivo LGTBIQ+— puede no aparecer mencionado en ningún momento del proceso algorítmico, así como tampoco cualquier tipo de referencia a la categoría sensible de orientación sexual del individuo.

Asimismo, aunque el trasfondo principal de la regulación de los datos sensibles sea evitar que los mismos se traten con efectos adversos o discriminatorios, los *proxies* presentan una particularidad, y es que su uso discriminatorio no tiene por qué caer en las definiciones tradicionales de discriminación directa o discriminación indirecta, sino que lo habitual será que su uso con fines publicitarios derive en la conocida como «discriminación por asociación», introducida por el TJUE en los casos *Coleman* y *CHEZ*[75][76]. Conforme a la discriminación por aso-

---

[72] Speicher, T. *et al.,* «Potential for Discrimination in Online Targeted Advertising», *Journal of Machine Learning Research*, 2018, pp. 14-15.

[73] Celis, E. *et al,* «Toward Controlling Discrimination in Online Ad Auctions», International Conference on Machine Learning, unpublished, 2019.

[74] Wachter, S. «Affinity profiling and discrimination…», *op. cit.*

[75] La discriminación directa tiene lugar cuando las decisiones discriminan explícitamente a los miembros de un grupo especialmente protegido, ocupándose de proteger la igualdad formal en la medida en que se centra en asegurar que ninguna decisión privilegie a un grupo sobre a otro sobre a base de un motivo protegido. *Vid.* Soriano Arnanz, A. «Discriminación algorítmica: garantías y protección jurídica», en Cotino Hueso, L (dir.) *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, 2022, pp. 139-166.

[76] Aunque la discriminación sea el trasfondo de la protección reforzada de los datos sensibles, el lector, en este punto, podría plantear por qué estamos tratando la discriminación como trasfondo de la protección de datos y no como vía directa —es decir, a través acciones por discriminación— para paliar dichas prácticas comerciales. Si bien es una vía perfectamente razonable, hemos decidido centrarnos en la perspectiva de la protección de datos por dos razones principales. La primera es que las acciones por discriminación se enfrentan a difíciles requisitos

ciación, no es necesario que el sujeto afectado pertenezca a un grupo protegido, sino que basta con que presente similitudes o afinidades con el mismo y que esta afinidad resulte en un trato discriminatorio[77]. La discriminación por asociación puede tener una fuerte presencia en los *proxies* y algoritmos publicitarios, ya que, para la personalización segmentada de la misma, no es necesario que el individuo pertenezca a un determinado grupo (por ejemplo, mujeres), sino que es suficiente con que se comporte de manera similar para que reciba los anuncios destinados a ese grupo (por ejemplo, anuncios de zapatos para mujeres)[78].

Aunque, como hemos señalado, en sede de protección de datos no es necesario que la práctica comercial personalizada derive en efectos adversos o discriminatorios, la potencial o actual concurrencia de éstos puede ser relevante. Así, ya en 2011, algunos Estados miembros propusieron al Grupo de Trabajo del Artículo 29 que el contexto y propósito de los datos sensibles debería considerarse al examinar si los datos presentan la naturaleza de datos sensibles[79]. Extender la protección de los datos sensibles a los *proxies* puede plantearse como necesario, si se justifica que los *proxies* utilizados en cuestión actúan funcionalmente como datos sensibles y, en consecuencia, pueden ser utilizados con fines discriminatorios.

Por esta razón, durante las siguientes páginas, expondremos diferentes argumentos para considerar los *proxies* como datos sensibles con base en las características y particularidades de cada una de las categorías de datos sensibles.

2.1. *Datos genéticos*

Los datos genéticos son una de las tres únicas categorías de datos sensibles definidas de forma expresa en el propio RGPD. Tales datos son conceptuados en el art. 4(13) como «aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis

---

probatorios, ya que es necesario probar un trato menos favorable por pertenencia o afinidad a un determinado grupo protegido. En cambio, en sede de protección de datos, no es necesario probar un daño o trato desfavorable, sino que basta con el incumplimiento de las normas de protección de datos, sin necesidad de que este incumplimiento derive en consecuencia alguna.

[77] Así, la discriminación directa también tiene lugar cuando una persona no perteneciente a un grupo especialmente protegido resulta directamente perjudicada por una decisión, conducta o medida debido a su relación con los miembros de un grupo protegido. *Vid.* Soriano Arnanz, A. «Discriminación algorítmica…», *op. cit.,* pp. 139-166.

[78] Wachter, S. «Affinity profiling and discrimination…», *op. cit.*

[79] Article 29 Data Protection Working Party, «Advice paper on special categories of data ("sensitive data")», 2011, pp. 9-14.

de una muestra biológica de tal persona»[80]. El considerando 34 del Reglamento ofrece una definición algo más exhaustiva, al señalar que son datos genéticos «los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente».

Ciertos autores señalan que los datos genéticos —es decir, los datos procedentes del ADN codificante— son una variante de los datos de salud, si bien presentan ciertas particularidades que los hacen diferentes de los demás datos relacionados con la salud[81]. La primera particularidad es que se encuentran en todas las células del cuerpo, salvo los hematíes, que no tienen núcleo, y los gametos, que tienen la mitad. La segunda es que los datos genéticos son únicos, con la salvedad de los gemelos monocigóticos, y son inalterables, salvo aquellas mutaciones espontáneas o provocadas. La tercera es que son datos predictivos, en particular, en situaciones asintomáticas. La última y cuarta particularidad de los datos genéticos radica en que las características que revelan se comparten en diversa medida con la familia biológica y se transmiten en diverso grado a la propia descendencia[82].

El análisis de los datos genéticos puede tener usos muy positivos. Así, dada su potencialidad predictiva, pueden utilizarse en la llamada *medicina personalizada de precisión avanzada*, facilitando estrategias de acción preventiva y permitiendo implementar nuevos procedimientos de diagnóstico[83]. Estos usos son posibles gracias a los algoritmos de predicción basados en la minería de datos, que podrían revelar qué personas presentan una mayor proclividad a desarrollar una enfermedad grave en el transcurso de sus vidas. A título de ejemplo, hay estudios que afirman la existencia de 75 factores de riesgo genético asociados al alzhéimer, los cuales podrían ser analizados a través de la recolección masiva y estudio de datos genéticos[84].

Sin perjuicio de sus usos positivos, también debemos tener presente que los datos genéticos pueden ser una vía para revelar otras categorías de datos sensibles, como el origen racial o étnico, o los datos relativos

---

[80] *Vid.* Art. 4.13 RGDP.

[81] Romeo Casabona, C. M. «Datos genéticos (comentario al art. 4.13 RGPD) al art. 4.13 RGPD)», en Troncoso Reigada, A. *Comentarios al Reglamento General…, op. cit.,* pp. 697-707.

[82] *Ibid.*, p.698.

[83] *Ibid.*, p.670.

[84] Identifican 75 factores de riesgo genético asociados al alzhéimer. CE Noticias Financieras, 5 de abril de 2022.

a la salud en un sentido general, al revelar la proclividad del individuo a padecer una enfermedad grave[85]. En este caso, los datos genéticos estarían funcionando como *proxies* o indicadores de otros datos sensibles. El riesgo de que los datos genéticos puedan ser utilizados con fines discriminatorios es un factor que justifica por qué se incluyeron en el grupo de categorías especiales de datos, teniendo en cuenta que la discriminación genética está expresamente prohibida en el derecho primario de la UE, como señala la Carta en su art. 21. A nivel internacional, esta prohibición también se encuentra en el Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa[86] y en la Declaración Universal sobre el Genoma Humano y los Derechos Humanos de la UNESCO[87].

La consecuencia de incluir los datos genéticos en la categoría de datos sensibles radica en que su tratamiento está sometido a reglas más estrictas que analizaremos en posteriores apartados. Sin embargo, sí que cabe adelantar que encontramos bastantes excepciones en el caso de los datos genéticos. Así, por ejemplo, dichas reglas decaen cuando el tratamiento es necesario con fines de medicina preventiva o para cumplir determinados objetivos de seguridad y salud laboral, evaluación de la capacidad de trabajo, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión, participación y comunicación de los sistemas y servicios de asistencia sanitaria y social, o cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública[88]. Como medida de seguridad, se establece que, en todas estas excepciones, hay un deber de confidencialidad para quienes tengan acceso legítimo. Por otro lado, si asumimos que los datos genéticos son una subcategoría especial de datos relacionados con la salud, conforme a algunos autores, cabría afirmar que las reglas del RGPD para estos últimos serían de aplicación subsidiaria a los datos genéticos cuando no exista una disposición específica prevista para estos últimos[89].

Al ser el objeto de investigación de este trabajo el estudio del abuso de datos personales en la publicidad personalizada, cabe plantearnos, llegados a este punto, qué rol pueden desempeñar los datos genéticos en la publicidad personalizada. La respuesta puede ser variada. A título de ejemplo, las compañías aseguradoras tienen un interés especial

---

[85] Grupo de Trabajo del Artículo 29 Sobre Protección de Datos, «Documento de trabajo sobre datos genéticos», 2004.

[86] *Vid.* Art 11 del Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa.

[87] *Vid.* Art. 6 de la Declaración Universal sobre el Genoma Humano y los Derechos Humanos de la UNESCO.

[88] *Vid.* Art. 9 RGPD.

[89] Romeo Casabona, C. M. «Datos genéticos (comentario al art. 4.13 RGPD)…», *op. cit.,* p. 672.

en conocer los datos genéticos de sus asegurados, ya que —como hemos señalado— los datos genéticos tienen una gran potencialidad para la predicción de enfermedades. El acceso indebido a estos datos podría dar lugar a discriminaciones en ofertas de contratos de seguro con base a los datos genéticos del sujeto, particularmente, en torno al precio o excluyendo a determinados individuos de la recepción de anuncios sobre dichas ofertas. Igualmente, como hemos señalado, los datos genéticos pueden actuar como *proxies* para indicar otros datos sensibles, como el origen étnico, lo que puede dar lugar a que ciertos anuncios excluyan a determinados grupos étnicos. En el apartado destinado a los datos reveladores de la raza o la etnia desarrollaremos esta problemática con más profundidad.

2.2. *Datos biométricos*

Los datos biométricos son una de las categorías de datos que más preocupación suscitan en el legislador a causa de sus riesgos. Se ha señalado frecuentemente por la doctrina que su mera recolección ya plantea numerosos problemas, por lo que su regulación debería ser particularmente cautelosa[90]. En la actualidad, los datos biométricos se emplean en procedimientos automatizados de autenticación, comprobación e identificación, si bien en sus orígenes su utilización se limitaba al análisis de ADN y a la verificación de huellas digitales, especialmente en el ámbito criminal, donde tuvieron una importante incidencia tanto en la investigación penal y civil como en la prueba[91].

Conviene comenzar destacando que los datos biométricos pueden ser definidos desde dos ópticas: la perspectiva técnica y la perspectiva jurídica, las cuales no siempre coinciden en la práctica[92].

A nivel técnico, se reconoce una doble categorización de datos biométricos, según se refieran a características anatómico-físicas o a características relativas al comportamiento[93]. Las características anatómico-físicas, también denominadas estáticas, son las huellas dactilares, el iris, la retina, la forma de la mano, el ADN (especialmente el no codificante, ya que para el codificante la regla general será remitirse a los datos genéticos), o ciertos biomarcadores presentes en fluidos corporales como la sangre, o el reconocimiento facial. Por su parte,

---

[90] Kindt, E. J. «Having yes, using no? About the new legal regime for biometric data» *Computer Law and Security Review*, 34, 2017, pp. 523-538.

[91] Barona Vilar, S. «Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale», *Actualidad Jurídica Iberoamericana*, núm. 21, 2024, pp. 298-331.

[92] Jasserand, C. A. «Avoiding Terminological Confusion between the Notions of "biometrics" and "biometric Data": An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective», *International Data Privacy Law,* vol. 6, 1, 2015.

[93] Gómez Sánchez, Y. «Categorías especiales de datos personales…», *op. cit.*

las características relativas al comportamiento, o características dinámicas, son la letra y la firma manuscritas, la forma de caminar, los gestos, la forma de pulsar las teclas de un aparato o la voz[94].

Todas estas características presentan una sensible relación con los derechos fundamentales a la privacidad, la protección de datos y la no discriminación. A su vez, la transcendencia que pueden tener estas características en la publicidad basada en perfiles no es menor. Cada vez con más frecuencia, los algoritmos publicitarios son entrenados para analizar características como los gestos faciales, la voz, el iris o la frecuencia y rapidez de los clics, al ser datos potencialmente reveladores del estado de ánimo de los individuos, y sirven para determinar y predecir reacciones frente a determinados contenidos y comunicaciones comerciales[95]. Ciertos estudios ya muestran que a través de técnicas de IA se puede detectar en tiempo real el estado emocional del sujeto y ajustar las respuestas en consecuencia, lo que se conoce como *IA emocional*[96].

Las respuestas automatizadas con base al análisis de emociones dan lugar a no pocas inquietudes sociales. El Consejo de Europa ya alertó en 2019 de la existencia de sistemas *machine learning* que permiten no solo predecir las elecciones de los individuos, sino también influenciar las emociones, pensamientos y acciones, a veces incluso de forma subliminal[97]. A título de ejemplo, si se habilita la cámara y el micrófono de un videojuego *online*, a través de sistemas de IA se podría medir cuándo el usuario está más excitado o nervioso, analizando datos como la dilatación de las pupilas, el tono de voz, el sudor, los gestos faciales o la frecuencia de los clics. El sistema de IA, analizando este conjunto de datos, puede remitir al usuario unos anuncios u otros en los momentos en los que es más proclive a verse influenciado por la publicidad debido a factores como su estado emocional.

Ahora bien, aunque muchos de estos datos sean biométricos desde un punto de vista técnico, no tienen por qué serlo jurídicamente[98]. Es decir, aunque ciertas características de comportamiento —como los gestos faciales, la forma de pulsar las teclas o el tono de voz— sean consideradas datos biométricos desde una perspectiva técnica, para que presenten esta calificación jurídica deberán cumplir con ciertos requisitos normativos.

---

[94] *Ibid.*

[95] Tomassi, S. «Digital Services and algorithmic discrimination», *op. cit.,* pp. 37-50.

[96] Valcke, P., Clifford, D. y Dessers, V., «Constitutional Challenges in the Emotional AI Era» in Micklitz, H.W. *et al., Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2021, pp. 57-77.

[97] Council Of Europe's Committee Of Ministers, «Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes», 2019.

[98] Jasserand, C.A. «Avoiding Terminological Confusion…», *op. cit.*

La definición jurídica de los datos biométricos la aporta el art. 4 (14) RGPD, que los entiende como aquellos «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos». Esta definición coincide con la aproximación técnica que anteriormente planteábamos, si bien presenta una diferencia importante: para que tales características sean consideradas datos biométricos, deben haber sido sometidas a un tratamiento técnico específico que permita o confirme la identificación única de una persona física a través de ellas. En otras palabras, si el sistema técnico utilizado para el tratamiento no permite o confirma la identificación única de una persona física, las características biométricas no tendrán la consideración de datos biométricos y, por ende, no se someterán a su regulación específica.

Este requisito plantea dos controversias principales. La primera es el riesgo que puede plantear la mera recolección de datos personales biométricos, aunque inicialmente no se sometan a sistemas que permitan identificar únicamente al individuo. Una vez que la información es recolectada, concurre el riesgo de destinar los datos biométricos a usos distintos del propósito inicial[99]. Esta aproximación seguiría el denominado filo del riesgo, sobre la base del cual algunos autores sostienen la necesidad de aplicar reglas más exigentes al tratamiento de datos que revelen características biométricas.

La segunda controversia surge cuando los sistemas técnicos utilizados no permiten la identificación única del individuo, pero permiten otros usos cuya eticidad puede resultar controvertida. Este sería, por ejemplo, el caso de los sistemas de IA de reconocimiento de emociones. El Reglamento de IA categoriza tales sistemas como de *alto riesgo*, pero solo cuando se basen en datos biométricos[100]. Aunque para definir estos últimos el art. 3 (34) de la AIA no se remita al RGPD, la definición que hace de ellos es una indiscutible transposición *verbatim* del art. 4 (14) del RGPD, como bien reconocen los considerandos de la AIA, al señalar que la noción de datos biométricos de esta coincide con la del RGPD y debe interpretarse conforme a la misma[101].

La alusión a los datos personales biométricos puede tener su sentido en un intento del legislador por acudir a términos ya existentes en el acervo de la UE. Si el legislador hubiese prohibido meramente el uso de sistemas de IA de reconocimiento de emociones, podríamos

---

[99] Sumer, B. «When do the images of biometric characteristics qualify as special categories of data under the GDPR?: a systemic approach to biometric data processing», *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2022, pp. 1-6.

[100] Anexo iii, apartado 1.*c)* del AIA.

[101] Considerando (14) de la AIA.

encontrarnos ante la incertidumbre de qué debemos entender por tales, al tratarse de un término evidentemente amplio y subjetivo. El considerando 18 de la AIA señala que bajo la noción de sistemas de IA de reconocimiento de emociones se deben incluir «emociones o intenciones como la felicidad, la tristeza, la ira, la sorpresa, el disgusto, la vergüenza, la emoción, el desprecio, la satisfacción y la diversión». Señala que este término no incluye:

— «Los estados físicos, como el dolor o la fatiga, dando como ejemplo de exclusión del supuesto de hecho los sistemas utilizados en la detección del estado de fatiga de pilotos o conductores profesionales con el fin de prevenir accidentes».

— «La mera detección de expresiones, gestos o movimientos fácilmente aparentes, a menos que se utilicen para identificar o inferir emociones. Esas expresiones pueden ser expresiones faciales básicas, como fruncir el ceño o sonreír, o gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como levantar la voz o susurrar».

Como comentaremos más adelante, es frecuente la utilización de sistemas *deep learning* para inferir emociones mediante, precisamente, gestos faciales y expresiones, por lo que estos sistemas podrían quedar englobados dentro del supuesto de hecho.

La mera lectura de este considerando ya revela la controversia que puede rodear a los sistemas de reconocimiento de emociones si no nos remitimos a unos parámetros mínimamente objetivos. Por esta razón, entendemos que en el proceso de negociaciones de la AIA se decidiese incluir la referencia a los datos biométricos como *factor moderador*. Esta solución, si bien comprensible, queda lejos de ser perfecta: al remitirse a un término acuñado por el RGPD, traslada las lagunas, antinomias y deficiencias del mismo, conservando las divergencias entre la realidad técnica y la realidad jurídica que surgen al tratar datos biométricos.

Poniendo como referencia los sistemas de reconocimiento de emociones, concurre el riesgo de que nos encontremos ante sistemas de IA entrenados para reconocer las emociones de los sujetos y producir respuestas con base a datos biométricos, pero no para identificar de forma única a personas físicas[102]. En estos casos, tales sistemas no serán calificados *de alto riesgo*, al no basarse en datos biométricos en sentido jurídico, por lo que no se verán sometidos a ciertas normas específicas, como obligaciones de transparencia, evaluación de riesgos y registro.

[102] Czarnocki, J. «Will new definitions of emotion recognition and biometric data hamper the objectives of the proposed AI Act?», *International Conference of the Biometrics Special Interest Group (BIOSIG),* 2021.

Algunos estudios ya muestran que este riesgo, bajo el actual estado de la técnica, se ha convertido en una realidad.

El principal uso de datos biométricos para reconocer emociones lo encontramos en los videojuegos *online*. En un experimento llevado a cabo en 2020, se utilizaron sistemas de IA de aprendizaje automático para medir y analizar las emociones de los jugadores[103]. El sistema fue capaz de reconocer emociones de los jugadores como la ira, la anticipación, la alegría, la confianza, el miedo, la sorpresa, la tristeza y el disgusto. Sin embargo, el sistema no era capaz de decir nada sobre la identidad del jugador, porque ese no era su propósito. De acuerdo con la normativa actual, no se calificaría como un sistema de reconocimiento de emociones, porque el sistema de IA utilizado no permitía identificar de forma única a los individuos.

Multitud de estudios evidencian la misma problemática. En 2018 se desarrollaron experimentos en los que, en contextos de publicidad y comercio electrónico, se posibilitaba la detección en tiempo real de emociones humanas manifestadas a través del rostro mediante sistemas de *deep learning*[104]. El experimento trataba de identificar, en tiempo real, las cuatro emociones básicas (tristeza, felicidad, enfado y miedo) alimentando los sistemas de IA con imágenes faciales. Varios de los sistemas *deep learning* utilizados presentaban un alto porcentaje de acierto, como *Commercial Affdex CNN*, que manifestaba una precisión del 85,05 por ciento.

Estudios posteriores manifiestan igualmente la posibilidad de utilizar sistemas *deep learning* para reconocer emociones no solo a través del rostro, sino también a través de la voz, con tasas de acierto ya más elevadas que alcanzan el 97 por ciento de precisión[105]. Otro estudio, de 2023, proponía la posibilidad de usar ChatGPT como herramienta para construir prototipos de software de reconocimiento de emociones[106].

El hilo común de todos estos experimentos es que los sistemas *deep learning* son diseñados para medir las emociones y, en su caso, producir respuestas en consecuencia, pudiendo consistir éstas en par-

---

[103] Burak Alakus, T., Gonen, M. y Turkoglu, I. «Database for an emotion recognition system based on EEG signals and various computer games – GAMEEMO», *Biomedical Signal Processing and Control*, vol. 60, 2020.

[104] Kartali, A., Roglić, M., Barjaktarović, M., Đurić-Jovičić, M. y Janković, M. «Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches», *14th Symposium on Neural Networks and Applications (NEUREL)*, 2018, pp. 1-4.

[105] Vardhan, J. V., Kalyan Chakravarti, Y. y Chand, A. J. «Emotion Recognition by Facial Expressions and Speech Using Deep Learning», *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 2024, pp. 1-7.

[106] Hermanus, D. R. *et al.,* «Unveiling the Power of ChatGPT: Transforming Face Detection with AI and AR», *10th International Conference on ICT for Smart Society (ICISS)*, 2023.

ticular en la presentación de anuncios y contenidos personalizados, pero no para identificar de forma única al destinatario. Es decir, como el sistema de IA produce respuestas adaptadas en tiempo real, no es necesario que identifique a la persona física en cuestión, ya que simplemente será entrenado para asignar determinados outputs (como anuncios) a determinados inputs (expresiones faciales u ondas de voz que revelen un estado de ansiedad). Es más, desde el punto de vista del responsable del tratamiento, la clave radica en que no solo no es necesaria la identificación única del sujeto, sino que esta ni siquiera le es conveniente. Evitando la identificación podría eximirse de las normas relativas al tratamiento de datos biométricos, como el RGPD y ciertas previsiones de la AIA.

La regulación de los datos biométricos se complica todavía más, si cabe, al entrar en juego la cuestión de calificar (y proteger) los datos biométricos como datos sensibles. La aproximación del RGPD en lo referente a estos datos es compleja, ya que se divide en dos partes. Para que los datos biométricos sean considerados datos sensibles y se sometan a su régimen especial, deberán cumplir dos filtros.

Primero, deberán ser datos biométricos en el sentido técnico y jurídico del art. 4 (14) del RGPD. En otras palabras, deben ser: *a)* datos personales, es decir, relativos a una persona identificada o identificable; *b)* relativos a las características físicas, fisiológicas o conductuales de una persona física; *c)* que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos; y *d)* obtenidos a partir de un tratamiento técnico específico, como puede ser el tratamiento mediante sistemas de IA[107]. Así, por ejemplo, señala el considerando 51 del RGPD que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Por ende, la principal laguna del primer filtro radica en que quedan excluidas todas las características biométricas no sometidas a un tratamiento técnico específico que permita una identificación única, laguna que se lleva advirtiendo desde la entrada en vigor del RGPD.

Segundo, para que sean calificados como datos sensibles y, en consecuencia, les sea de aplicación su normativa específica, deberán estar «dirigidos a identificar de manera unívoca a una persona física», conforme exige el art. 9 (1) RGPD. La principal adición respecto a la definición anterior de datos biométricos es que no se exige meramente

[107] AEPD, «Guía sobre tratamientos de control de presencia mediante sistemas biométricos», 2023.

que el tratamiento *permita o confirme* la identificación única de una persona, sino que su tratamiento deberá estar *dirigido a* dicha identificación. Es decir, la identificación unívoca no solo debe ser posible, sino que debe ser el propósito mismo del tratamiento.

Este segundo filtro es bastante destacable, ya que los datos biométricos constituyen la única categoría en la que el RGPD se ha apartado de una definición contextual y ha incluido el propósito con el que deben ser tratados para ser considerados datos sensibles. A nuestro entender y el de muchos autores, la razón de esta divergencia radica en que el legislador comunitario quiso evitar que todas las fotografías e imágenes en las que aparezcan personas físicas caigan bajo la regulación *sui generis* de los datos sensibles, como bien confirma el considerando 51 del RGPD[108]. La inclusión de este propósito como requisito *sine qua non* para la protección especial de los datos biométricos ha dado lugar a amplias lagunas jurídicas.

Según la guía sobre tratamiento de datos personales a través de vídeo del CEPD, si un sistema no genera plantillas biométricas para identificar a personas físicas, sino que simplemente detecta características biométricas para clasificar a personas, no se estaría llevando a cabo un tratamiento de datos biométricos sensibles[109]. El CEPD pone como controvertido ejemplo el caso del dueño de una tienda que desee personalizar sus anuncios conforme al género y la edad de sus clientes captados por cámara. Según la guía, si el propósito del tratamiento no es identificar de forma única a los clientes, sino distinguirlos por categorías, estos datos en bruto (*raw data*) no serían datos biométricos sensibles, por lo que el art. 9 RGPD no sería de aplicación.

La anterior interpretación es profundamente criticada por parte de la doctrina, y, a nuestro entender, puede dar lugar a casuísticas enormemente problemáticas. Pongamos el caso de un sistema de IA de reconocimiento de emociones que sea entrenado para elaborar perfiles publicitarios conforme a características biométricas en sentido técnico, como imágenes de gestos faciales. Si siguiéramos la guía del CEPD podríamos considerar que estas imágenes no constituyen datos biométricos en el sentido del RGPD, ya que no han sido procesadas con el propósito de identificar de forma única a una persona, sino que el propósito era categorizarla.

Encontramos esta aproximación enormemente desacertada, ya que los perfiles individuales, *de facto*, identifican al sujeto con base a sus datos personales y, conforme a dicha identificación, le remiten una publicidad u otra. Que el responsable de datos afirme que el propósito del tratamiento sea categorizar y no identificar resulta un tecnicismo

---

[108] *Vid.* por todos. Malgieri, G. y Quinn, P. «The Difficulty of Defining…», *op. cit.*

[109] EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, p. 19.

irrelevante y, a nuestro entender, un posible caso de fraude de ley. La elaboración de perfiles publicitarios, especialmente de perfiles individuales en tiempo real, se basa en el tratamiento automatizado de datos personales de destinatarios concretos, siendo imprescindible la identificación. Depender totalmente del propósito teórico declarado por el responsable de tratamiento implicaría que el requisito de *identificación única* se utilice como una vía de escape excesivamente amplia.

Sin embargo, si quisiéramos alentar las bondades de esta cláusula de escape, bajo una interpretación literal de la norma podría argumentarse que en la elaboración de perfiles publicitarios no se produce una identificación *única* de la persona, ya que la publicidad personalizada conlleva siempre un margen de error respecto a las características atribuidas a un usuario, a veces derivado del riesgo de que un mismo dispositivo sea utilizado por más de un individuo o de sesgos en el sistema algorítmico. En estos casos, la clave radicará en qué margen de error es aceptable para entender que el propósito es la identificación *única.*

Teniendo en cuenta la gran incertidumbre que rodea la calificación como sensibles de los datos biométricos, proponemos como alternativa práctica comprobar si los datos en cuestión son encuadrables en otras categorías de datos sensibles. Siguiendo el ejemplo anterior, las imágenes del rostro de un sujeto pueden ser reveladoras de otros tipos de datos sensibles, como el origen étnico. No en vano el art. 9.1 del RGPD considera como categorías especiales de datos aquellas que *revelen* cierto tipo de información. Es señalado por una gran parte de la doctrina que los datos biométricos son particularmente reveladores de otros tipos de datos sensibles[110]. Concluyen algunos autores, con los que nos encontramos de acuerdo, que la interpretación de los datos biométricos como categorías especiales de datos debe tener en cuenta la posibilidad de que, mediante el análisis biométrico, se puedan inferir y recoger otras categorías especiales de datos y, en particular, datos relativos a la salud o que revelen el origen racial o étnico, entre otros. A título de ejemplo, algunos *sistemas deep learning* ya están siendo utilizados para detectar enfermedades de piel a través de imágenes del rostro[111]. Aunque dichas imágenes no fuesen datos biométricos en el sentido del RGPD (al no ser utilizadas con el propósito de identificación única), seguirían siendo datos sensibles, ya que revelan datos relativos a la salud.

Concluyendo, esta aproximación alternativa daría lugar a que cierta normativa —como la prohibición de la DSA de presentar publicidad basada en perfiles utilizando datos sensibles— sea de aplicación

---

[110] Kindt, E. *Privacy and data protection issues of biometric applications. A comparative legal analysis*, Springer, 2013.

[111] Kumar, A. Shetty, P., Balipa, M., Rao, B., Puneeth, B. And Shravya, «An efficient technique to detect skin Disease Using Image Processing», *2022 International Conference on Artificial Intelligence and Data Engineering (AIDE)*, 2022., pp. 35-40.

aun cuando los datos no cumplan con los requisitos para ser datos sensibles biométricos, pero sí revelen otros datos sensibles. Sin embargo, como veremos más adelante, seguimos encontrándonos ante una solución imperfecta, ya que las demás categorías de datos sensibles presentan sus exigencias propias, excluyendo asimismo categorías de datos que no son protegidas como datos sensibles por no encontrarse en la lista cerrada del art. 9 RGPD.

2.3. *Datos relativos a la salud*

Los datos relativos a la salud son la tercera categoría de datos sensibles definida en el RGPD. A diferencia de los datos genéticos y los datos biométricos, los datos relativos a la salud ya se mencionaban en la DPD. En la práctica, tanto en la actividad asistencial como epidemiológica se ha evidenciado la importancia del acceso a este tipo de datos, sobre todo tras la pandemia del COVID-19, así como la necesidad de asegurar un sistema de garantías suficientes para proteger la privacidad sobre estos datos[112].

El RGPD define los datos relativos a la salud como aquellos datos personales «relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud»[113]. Esta definición, de carácter evidentemente amplio, resulta un poco más detallada en los considerandos del RGPD. Estos afirman que bajo esta categoría se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental, pudiendo esta información recaer sobre el estado de salud pasado, presente o futuro[114].

A nuestro entender y el de otros autores, era necesaria la inclusión de los datos sobre el estado de salud futuro, habida cuenta, especialmente, de la información predictiva que pueden aportar los datos genéticos y la detección de ciertos biomarcadores presentes en el cuerpo del paciente[115]. Señalan igualmente los considerandos —bajo una sintaxis un tanto farragosa— que se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de confor-

---

[112] Oliveira Hashiguchi, T. C., Slawomirski, L. y Oderkirk, J. «Laying the foundations for artificial intelligence in health», *OECD Health Working Papers*, núm. 128.

[113] *Vid.* Art. 4.15 RGPD.

[114] *Vid.* Art. 4.15 RGPD.

[115] *Vid.* Por todos. Romeo Casabona, C. M. «Datos relativos a la salud (comentario al art. 4.15 RGPD)», en Troncoso Reigada, A. *Comentarios al Reglamento General…, op. cit.,* pp. 715-731.

midad con la Directiva 2011/24/UE[116]. Esta información incluye todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente[117]. Entre las posibles fuentes, los considerandos mencionan a un médico u otro profesional sanitario, un hospital, un dispositivo médico o una prueba diagnóstica *in vitro*[118].

Una primera lectura evidencia el carácter abierto del concepto de datos relativos a la salud, amplitud del concepto que ha sido destacada por la propia jurisprudencia del TJUE. Así, en el caso *Lindqvist*, el Alto Tribunal adoptó una interpretación amplia de la expresión «datos relativos a la salud» para incluir la información relativa a todos los aspectos, tanto físicos como mentales, de la salud de una persona[119]. En el caso *Vyriausioji tarnybinės etikos komisija*, el Alto Tribunal se mantuvo igualmente a favor de un entendimiento amplio, al señalar «para que los datos personales sean calificados de datos relativos a la salud […] basta con que tengan la naturaleza de revelar, a través de una operación intelectual de conciliación o deducción, información sobre el estado de salud del interesado», posición que ha sido reiterada en el caso *Lindenapotheke*[120][121].

Ahora bien, subsisten ciertas controversias en torno a cómo de amplia debe ser la interpretación del concepto de datos relativos a la salud. Desde el punto de vista de la publicidad personalizada, no es en absoluto trivial cuestionar si los *proxies* —en este caso, datos indicadores del estado de salud actual o futuro— deben gozar de la misma protección que los datos relativos a la salud y ser considerados equivalentes a éstos. Afirmamos que no es una cuestión banal ya que, dependiendo de la respuesta, el régimen jurídico aplicable será notablemente distinto, especialmente si el fin del tratamiento es la publicidad basada en perfiles.

---

[116] Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

[117] *Vid.* Art. 4.15 RGPD.

[118] *Vid.* Art. 4.15 RGPD.

[119] Conforme al Tribunal, la referencia al hecho de que una persona se había lesionado un pie y trabajaba a media jornada por motivos médicos constituía un dato personal relativo a la salud en el sentido de la DPD. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, *Bodil Lindqvist*, asunto C-101/01, (ECLI:EU:C:2003:596).

[120] Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de agosto de 2022, *OT y Vyriausioji tarnybinės etikos komisija*, asunto C-184/20 (ECLI:EU:C:2022:601).

[121] Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de octubre de 2024, *Lindenapotheke*, asunto C-21/23 (ECLI:EU:C:2024:846).

La envergadura de este problema puede comprenderse fácilmente si lo abordamos desde un enfoque causal. Existe una miríada de ejemplos en los que el algoritmo publicitario detecta ciertos *proxies* que circunstancial e indirectamente pueden aportar información relativa al estado de salud de un individuo. A través de la dirección IP del dispositivo, el algoritmo puede conocer su lugar de residencia, el cual puede ser relevante, ya que multitud de estudios revelan que el entorno medioambiental afecta a las condiciones de salud. Así, vivir en una ciudad con altos niveles de contaminación puede incrementar las posibilidades de cáncer, al contrario que vivir en una zona rural[122]. La geolocalización también puede actuar como un *proxy* de hábitos alimentarios poco saludables, ya que muestra los restaurantes que el usuario frecuenta. Igualmente, el historial de búsquedas puede mostrar la probabilidad de que el individuo se encuentre enfermo. Los especialistas alertan de que cada vez es más frecuente la búsqueda de síntomas en Google, búsqueda que da lugar a conclusiones poco fiables[123].

Por otro lado, los dispositivos inteligentes conectados al Internet de las cosas (IoT) también recopilan una cantidad importante de *proxies* sobre el estilo de vida. A diario, los relojes inteligentes pueden detectar cuánto deporte realiza el usuario, dato que, indirectamente, revela información relativa al posible estado de salud del individuo. Igualmente, los relojes inteligentes detectan otros *proxies*, como las horas de sueño o las pulsaciones, que presentan una conexión todavía más estrecha con la salud. Podríamos discutir si el carácter de todos estos *proxies* es estrictamente relativo a la salud, aunque lo que no resulta discutible, desde un punto de vista funcional, es que pueden ser utilizados por empresas publicitarias y aseguradoras para realizar un juicio provisional sobre el estado de salud del individuo y, en consecuencia, construir un perfil de cada individuo para diseñar los anuncios y ofertas comerciales que se le dirigirán.

Ateniéndonos a la regulación actual, podemos acudir a diversos métodos interpretativos para determinar si los *proxies* pueden ser datos relativos a la salud. Bajo una interpretación literal del art. 9 (2) RGPD, la misma formulación del término, *datos relativos a la salud*, revela que deben estar relacionados con o ser referentes a la salud, pero la expresión no presenta alcance restrictivo ya que, de lo contrario, podría haberse optado por el término *datos de salud* o *datos sobre salud*. En la versión en inglés del RGPD, el término utilizado es *personal data concerning health*, que no *personal health data*, lo que confirma la amplitud del término. En la versión en francés del texto, el concepto

---

[122] Vargas Marcos, F. «La contaminación ambiental como factor determinante de la salud», *Revista española de salud pública*, 2005, pp. 117-127.

[123] Balado, L. «¿Buscas tus síntomas en Google? “El problema es que uno encuentra lo que quiere encontrar”», *La Voz de Galicia*, 2022.

utilizado es *données concernant la santé,* que no, por ejemplo, *données de santé,* lo cual también revela la flexibilidad del precepto.

Bajo una interpretación contextual, si nos remitimos a los considerandos del RGPD, podemos apreciar cómo el legislador no establece una lista taxativa de datos relativos a la salud o de fuentes de estos, al añadir la expresión abierta «y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente»[124]. Así, se revela la intención del legislador comunitario de que el Reglamento se adapte a los continuos cambios científicos, siguiendo el principio de neutralidad tecnológica, y de ofrecer una protección amplia a estos datos relativos a la salud.

Bajo una interpretación teleológica, la finalidad perseguida al establecer una regulación *sui generis* de los datos relativos a la salud es la de ofrecer una amplia protección a los derechos y libertades fundamentales que pudieran verse implicados, como el derecho fundamental a la privacidad, y evitar efectos adversos como la discriminación. Si atendemos a la finalidad de la norma, por ende, el concepto de datos relativos a la salud debe ser un concepto amplio, para evitar que ciertos datos relativos a la salud puedan ser tratados sin que operen las garantías que otorga el RGPD.

Siguiendo una interpretación funcional del precepto, algunos autores ya alzan la voz abogando por que los *proxies* —denominados por ellos como *datos circunstanciales, funcionales o indirectos*— puedan ser considerados datos relativos a la salud, en la medida en que estos datos se encuentren vinculados de forma permanente o temporal con estos últimos y sean utilizados con propósitos o en contextos relacionados con la salud[125]. Ante este argumento nos encontramos de acuerdo solo parcialmente. Entendemos que los factores mencionados deberían ser entendidos como indicadores y no como requisitos cumulativos para que los datos personales inferidos sean considerados datos relativos a la salud. Si interpretamos que deben ser requisitos cumulativos, estaríamos atendiendo a una interpretación menos garantista, con más riesgos de vías de escape para prácticas que pueden llegar a ser discriminatorias. A título de ejemplo, si la norma exigiese que, en todo caso, el propósito deba estar relacionado con la salud, ciertos tipos de comunicaciones comerciales escaparían a esta obligación. Así, si el algoritmo publicitario de un videojuego detecta que el usuario es adicto al mismo, podría no considerarse la adicción como un dato relativo a la salud si exigimos que el propósito esté relacionado con la

[124] *Vid.* Considerando (35) RGPD.

[125] Romeo Casabona, C. M. «Datos relativos a la salud…», *op. cit.*

salud, dejando fuera el propósito de emitir publicidad sobre el servicio (el videojuego). Ahora bien, si los requisitos no son cumulativos, basta con que los *proxies* revelen información sobre el estado de salud (una adicción) para que sean considerados datos sensibles, independientemente de si son usados con propósitos o en contextos relacionados con la salud.

En contraposición, otros autores señalan que los datos relativos a la salud deben recibir una protección reforzada debido a la información que revelan o que pueden llegar a revelar, y no en función del fin objeto del tratamiento[126]. Este planteamiento puede resultar útil cuando analizamos datos personales individualmente, pero puede resultar más confuso cuando es el conjunto de *proxies* el que revela información relativa a la salud. Por ejemplo, el lugar de residencia, por sí solo, puede no ser revelador de datos sobre salud, sino que es el conjunto de este dato personal con otros —como el deporte realizado, las horas de sueño y los hábitos alimenticios— lo que permite revelar datos o conclusiones sobre el posible estado de salud —presente o futuro— del sujeto de datos. En este escenario, sí que es útil que consideremos como indicio que los datos se encuentren vinculados de forma permanente o temporal con datos relacionados con la salud, o que sean utilizados con tales propósitos o en contextos vinculados.

En consecuencia, bajo una interpretación funcional, sostenemos que los *proxies* pueden ser datos relativos a la salud si, por sí mismos o en conjunto, revelan aspectos referentes al estado de salud de un sujeto, siendo relevante pero no imperativo que tales datos sean utilizados con propósitos o en contextos relacionados con la salud. Por otra parte, añadiríamos que dichos *proxies* deben tener la capacidad de identificar o hacer identificable al sujeto pues, de lo contrario, la normativa de protección de datos no sería de aplicación, ya que los datos tratados no serían datos personales. En el caso de los objetos inteligentes, resulta sencillo que se cumpla el requisito de la identificación, ya que exigen que el usuario cree una cuenta en la *app* del dispositivo o que acceda a través de su perfil en una red social —lo que ya implica cesión de datos a terceros—. Igualmente, dichos dispositivos necesitan acceso a una red, por lo que la dirección IP del *router* también facilitará que el individuo sea identificable.

Otro posible indicador, como señalábamos, es que los *proxies* sean utilizados con propósitos o en contextos relacionados con la salud. Si un usuario utiliza un reloj inteligente de Amazon, sería normal que no se sienta igual de cómodo si los datos son utilizados solo para remitirle alertas o si el mismo Amazon los comparte con aseguradoras a las que vende los datos de los usuarios. Si realizamos una interpre-

[126] Gómez Sánchez, Y. «Categorías especiales de datos personales…», *op. cit.*

tación totalmente restrictiva de los datos sobre salud —reduciéndolos a datos sobre enfermedades o tratamientos—, estaríamos vaciando de contenido el propósito mismo de la regulación, ya que eliminaríamos de la ecuación a una cantidad masiva de datos que pueden perjudicar a las personas físicas por el mero hecho de que no revelen clara o directamente el estado de salud del individuo.

Por otro lado, conviene apuntar que ciertos aspectos relativos al tratamiento de datos de salud sufrirán cambios una vez entre en vigor el EEDS. Si bien el análisis de esta norma excede el propósito de este trabajo, conviene señalar que la misma contiene previsiones dirigidas a evitar el uso de datos relativos a la salud con fines que puedan resultar en efectos adversos para los sujetos de datos[127]. Pese a que, como veremos más adelante, los datos relativos a la salud pueden ser tratados bajo ciertas condiciones conforme al RGPD, la propuesta de EEDS es mucho más estricta. Así, la nueva norma parte de la prohibición de acceso a los datos de salud para tomar decisiones perjudiciales para una persona física sobre la base de sus datos electrónicos de salud, excluirla del beneficio de un contrato de seguro o modificar sus contribuciones y primas de seguro[128]. En el ámbito publicitario, la propuesta prohíbe utilizar los datos relativos a la salud obtenidos para dedicarlos a actividades publicitarias o de marketing dirigidas a personas físicas[129].

Pese a que dicha prohibición solventaría muchos de los problemas que aquí planteamos, no debemos olvidar que esta se circunscribe al ámbito de aplicación de la propuesta de EEDS, por lo que solo sería relevante en aquellos casos en los que el acceso a los datos de salud se realice a través del Espacio Europeo de Datos Sanitarios. El resto de los casos, en los que los datos relativos a la salud no se obtuvieron mediante una autorización conforme al EEDS, escaparían de la prohibición.

2.4. *Datos reveladores del origen étnico o racial*

La primera categoría de datos sensibles no definida por el RGPD son los datos reveladores del origen étnico o racial. Este tipo de datos sí se menciona en los considerandos del Reglamento, al enfatizar la especial protección de los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales, debiendo incluirse entre tales datos los datos de carácter

---

[127] Para un análisis más exhaustivo del EEDS en otro lugar, puede consultarse Sánchez Frías, I. «Secondary uses of health data under the European Health Data Space: connections with the GDPR and the impact of AI», *Revista General de Derecho Europeo,* núm. 65, 2025, pp.212-231.

[128] Art. 35 EEDS.

[129] Art. 35 EEDS.

personal que revelen el origen racial o étnico[130]. La inclusión de esta categoría es totalmente coherente con los principios y políticas que rigen el acervo internacional. La Carta de los Derechos Fundamentales de la UE prohíbe toda discriminación por razón de raza y orígenes étnicos[131]. Por otro lado, la lucha contra la discriminación por tales motivos es una de las acciones integradas en el TFUE[132]. Igualmente, en el ámbito del Consejo de Europa, el CEDH establece que «el goce de los derechos y libertades reconocidos en el Convenio ha de ser asegurado sin distinción alguna, especialmente por razones de raza, origen nacional o social, o cualquier otra situación»[133].

Desde un punto de vista científico, el concepto de *raza* puede resultar criticable, ya que, como señaló el Grupo de Trabajo del Artículo 29 «el homo sapiens no se divide hoy en día en diferentes razas ni subtipos»[134]. Por esta razón, los considerandos del RGPD afirman que la utilización del término *origen racial* en el Reglamento no implica una aceptación por parte de la Unión de teorías que intenten determinar la existencia de razas humanas separadas[135]. Podría plantearse entonces qué implica la inclusión de este término en la categoría de datos sensibles. Algunos autores señalan que el término *raza* abarca información como la pertenencia a una minoría y el color de la piel[136]. La RAE incluye varias acepciones, entre las cuales encontramos la definición de raza como «casta o calidad del origen o linaje» o «cada uno de los grupos en que se subdividen algunas especies biológicas y cuyos caracteres diferenciales se perpetúan por herencia».

La Comisión Europea ha publicado algunos informes y guías arrojando algo de luz respecto al concepto de origen racial o étnico[137][138]. Lo más destacado de estos documentos quizás radica en el enfoque de este término como una categoría conceptual única, integral y transversal, utilizada para la aplicación del derecho antidiscriminatorio y como una base jurídica valiosa para la interpretación legal, especialmente en el contexto actual, caracterizado por la falta de definiciones claras. Conforme al informe, los orígenes raciales, étnicos y nacionales son conceptos mutables, que comprenden la nacionalidad, el color, la ascendencia, la religión minoritaria, el idioma minoritario, la cultu-

---

[130] *Vid.* Considerando 51 RGPD.

[131] *Vid.* Art. 21.1 de la Carta de los Derechos Fundamentales de la UE.

[132] *Vid.* Art. 19 TFUE.

[133] *Vid.* Art. 14 CEDH.

[134] Ludmila, G. y Kuner, C. «Article 9 Processing of special…», *op. cit.,* pp. 365-385.

[135] *Vid.* Considerando 51 RGPD.

[136] Ludmila, G. y Kuner, C. «Article 9 Processing of special…», *op. cit.,* pp. 365-385.

[137] European Commission, Directorate-General for Justice and Consumers y Farkas, L., «Analysis and comparative review of equality data collection practices in the European Union – Data collection in the field of ethnicity», *Publications Office*, 2017.

[138] European Commission, «Guidance Note on the collection and use of equality data based on racial or ethnic origin», *Publications Office*, 2021.

ra y las tradiciones minoritarias[139]. Señala igualmente el informe que, junto con la extranjería y la inmigración, estas características constituyen los indicadores más comunes del origen racial o étnico, lo que se confirma más claramente en el contexto de la recopilación de datos sobre las desigualdades, que se basa decididamente en estos *proxies*[140].

Aunque tales documentos de la Comisión Europea no presentan carácter vinculante, resultan de gran valor a nivel interpretativo, ya que, en caso de duda, ofrecen una visión amplia más garantista para la protección de los sujetos de datos. A pesar de que la lista de datos sensibles que ofrece el RGPD es una lista cerrada, el hecho de que la Comisión reconozca que datos como la nacionalidad o el idioma pueden ser indicadores del origen racial o étnico nos permite, bajo una interpretación contextual, sostener la tesis de que los *proxies* pueden ser datos sensibles y someterse a su especial regulación. Igualmente, bajo una interpretación teleológica, el sentido de la regulación *sui generis* de los datos reveladores del origen étnico o racial es evitar la discriminación y otros efectos adversos por el uso de estas categorías especiales de datos. Si los *proxies* son utilizados con fines adversos o discriminatorios —veremos algunos casos a continuación— razón de más para afirmar que presentan la naturaleza jurídica propia de los datos sensibles.

En el ámbito de la publicidad personalizada, el abuso de datos reveladores del origen étnico o racial puede llegar a tener consecuencias graves. De hecho, si tomamos como referencia el caso de *Cambridge Analytica*, podemos afirmar que dichas consecuencias ya han comenzado a manifestarse. Algunos estudios muestran que Cambridge Analytica utilizó datos —obtenidos de Facebook y otras empresas— que revelaban los orígenes étnicos de los votantes para influenciar las votaciones nacionales de 2015 de Trinidad y Tobago[141]. Tal influencia se realizó a través de anuncios y contenidos en redes[142]. Por otro lado, un antiguo trabajador de Cambridge Analytica, Christopher Wylie, afirmó que durante la campaña a favor del Brexit la empresa ayudó a fomentar contenidos y anuncios que exacerbaban el racismo y que solo iban dirigidos a ciertos grupos seleccionados de personas blancas[143].

Los ejemplos en el ámbito publicitario no son escasos. Ya en 2016, *ProPublica* publicó una serie de informes que revelaban que Facebook permitía a los anunciantes excluir a ciertos grupos —como «negros,

---

[139] European Commission, Directorate-General for Justice and Consumers y Farkas, L., «Analysis and comparative…», *op. cit.*

[140] *Ibid.*

[141] Oddleifson, E. «The effects of modern data analytics in electoral politics: Cambridge Analytica's Suppression of Voter Agency and the implications for global politics», *Political Science Undergraduate Review*, 2020 pp. 46-52.

[142] *Ibid.*

[143] Perrigo, B. «"The Capabilities Are Still There". Why Cambridge Analytica Whistleblower Christopher Wylie Is Still Worried», *TIME*, 2019.

hispanos y etnias afines»— de anuncios sobre alojamiento, empleo o contratos de crédito basándose en la etnia[144]. En el caso de anuncios sobre alojamiento, el informe mostraba cómo Facebook ofrecía un cuestionario a los anunciantes para elegir a qué tipo de usuarios querían dirigirse, y bajo un apartado denominado «demografía/afinidad étnica», aportaba la opción de excluir a usuarios hispanos, afroamericanos y asiático-americanos.

El gerente de la política de privacidad de Facebook respondió a la controversia afirmando que las políticas de Facebook prohíben usar las opciones de personalización para discriminar, ofreciendo el dudoso argumento de que los anunciantes tenían la posibilidad tanto de incluir como de excluir a ciertos grupos con el objeto de comprobar cómo de bien funcionaba la campaña, siendo esto «una práctica habitual en la industria». El gerente justificó la categoría de *afinidad étnica* como un esfuerzo para fomentar la publicidad multicultural.

Aunque Facebook anunció en 2019 que iba a cambiar su política, no permitiendo que los anuncios de alojamiento, empleo o préstamos puedan dirigirse a grupos basándose en la raza, etnia, orientación sexual o religión, algunas preocupaciones subsisten, ya que Facebook continúa permitiendo que los anunciantes creen audiencias personalizadas basándose en el *Píxel* de Meta, el cual revela multitud de *información personalmente identificable* (PII)[145]. El Píxel de Meta es un código JavaScript inserto en la página web del anunciante. Este código le permite entender mejor la eficacia de sus anuncios, así como las acciones que los destinatarios llevan a cabo, como visitar una página o añadir un artículo al carrito. También le permite saber cuándo los clientes realizaron una acción después de haber visto su anuncio en Facebook o Instagram, lo que puede servir para volver a segmentar el anuncio de una forma más eficiente[146]. Ahora bien, esta segmentación o personalización de la audiencia permite a los anunciantes incluir o excluir a sujetos en función de una gran variedad de datos. Entre estos datos encontramos la localización, los viajes realizados, el tiempo dedicado en una red social, la educación, las páginas visitadas, el estado civil, si el usuario tiene una relación, los ingresos, y la afiliación política, pudiendo también segmentar conforme a la localización. Toda esta amalgama de datos sigue pudiendo utilizarse para identificar a cada usuario como perteneciente a uno o varios grupos.

Pese a las posibles justificaciones que pueda exponer la red social, la realidad es que, con base a *proxies* reveladores de origen racial o étnico, muchas personas pueden no tener acceso a ciertas ofertas

---

[144] Parris, T. y Angwin, J. «Facebook lets advertisers exclude users by race», *ProPublica,* 2016.

[145] Wachter, S. «Affinity profiling and discrimination…», *op. cit.*

[146] Facebook para empresas, «¿Qué es el Píxel de Meta?».

y anuncios. Este sesgo limita su capacidad de decisión, ya que el repertorio de opciones que se le plantean quedará enormemente limitado, todo ello sin dejar de lado el carácter eminentemente discriminatorio de tales prácticas comerciales. Estos riesgos ya manifestados no hacen sino evidenciar la necesidad de integrar una interpretación funcional de los datos sensibles, en la que el propósito, el contexto y la vinculación temporal o permanente de los *proxies* sean tenidos en cuenta para considerar la naturaleza sensible de los mismos a efectos de la normativa de protección de datos.

2.5. *Datos reveladores de opiniones políticas*

Otra categoría de datos sensibles son los datos reveladores de opiniones políticas. La tipificación de esta categoría se suele relacionar con la no interferencia en la libertad de expresión[147], protegida por la Carta de los Derechos Fundamentales de la UE[148] así como por el Convenio Europeo de Derechos Humanos[149]. Igualmente, aunque la protección de los datos reveladores de opiniones políticas tiene una clara conexión con la libertad de expresión, añadiríamos que el origen de la protección de estos datos también se encuentra en el principio de no discriminación, ya que los mismos pueden ser utilizados para construir perfiles de los sujetos o categorizarlos como afines a un grupo, resultando en efectos manipulativos o discriminatorios. En España, la Constitución proclama el derecho fundamental a la «libertad ideológica, religiosa y de culto» añadiendo la prohibición de que «Nadie podrá ser obligado a declarar sobre sus ideologías, religión o creencias». De este modo, operan dos grandes ámbitos de protección respecto del libre pensamiento, uno cimentado sobre un fundamento político y otro con base religiosa o filosófica[150].

Respecto a qué datos comprenden los datos reveladores de opiniones políticas, es comúnmente aceptado que pueden incluir, por ejemplo, la afiliación a un partido político, la participación en manifestaciones y las declaraciones o publicaciones políticas[151]. Sin embargo, más allá de estas expresiones activas, en la era *Big Tech*, las opiniones y tendencias políticas de cada individuo pueden ser detectadas no solo por acciones como las anteriores, sino también por su comportamiento *online* y por predicciones basadas en el mismo. Entre el comportamien-

---

[147] Ludmila, G. y Kuner, C. «Article 9 Processing of special…», *op. cit.,* pp. 365-385.

[148] *Vid.* Art. 11 de la Carta de los Derechos Fundamentales de la UE.

[149] *Vid.* Arts.9 y 10 CEDH.

[150] Rebollo Delgado, L. «Las condiciones de tratamiento de categorías especiales de datos (comentario al art. 9 RGPD y al art. 9 LOPDGDD», en Troncoso Reigada, A., *Comentarios al Reglamento General*, *op. cit.,* pp. 1013-1039.

[151] Ludmila, G. y Kuner, C. «Article 9 Processing of special…», *op. cit.,* pp. 365-385.

to *online* que puede revelar las opiniones políticas del usuario podemos encontrar, por ejemplo, la visita a páginas web, seguir la cuenta oficial de un partido político o de sus representantes en redes sociales o inscribirse en eventos de partidos a través de dichas redes.

El papel de los datos reveladores de opiniones políticas ha sido fundamental para disparar la preocupación internacional en cuanto al uso de técnicas de microsegmentación de la población con fines publicitarios o propagandísticos. De forma particular, los riesgos que plantea para la democracia el uso de datos reveladores de ideas políticas se manifestaron catastróficamente tras el escándalo de *Cambridge Analytica*. En 2018, el Comité Selecto sobre Digital, Cultura, Medios de Comunicación y Deporte de la Cámara de los Comunes de Reino Unido publicó un informe sobre las noticias falsas (*fake news*)[152]. Este informe reflejó cómo una consultora especializada en recolección y análisis de datos, llamada Cambridge Analytica, había utilizado los datos personales de unos 200 000 usuarios de Facebook para elaborar perfiles psicológicos detallados de hasta 87 millones de usuarios de la red social.

El primer gran problema radicó en que, aunque los 200 000 usuarios habían completado voluntariamente el test de personalidad, no sabían cómo se utilizarían sus respuestas y los 87 millones de usuarios a los que se elaboró el perfil no habían dado su consentimiento informado para ello[153] [154]. El segundo gran problema fue que los perfiles construidos se destinaron, entre otros usos, a determinar qué usuarios eran *votantes indecisos*. Gracias a la recolección y análisis de esta base de datos masiva, Cambridge Analytica interfirió en campañas políticas en el Reino Unido —la campaña a favor del Brexit—, Estados Unidos —las elecciones de 2016 en las que Donald Trump ganó la presidencia— y otros países —como Trinidad y Tobago— para dirigirse a los

---

[152] Dcms Comittee, «Disinformation and "fake news"», 2018.

[153] Heawood, J. «Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal», *Information Polity*, 2018.

[154] Este test de personalidad seguía la denominada escala OCEAN, anagrama de una teoría formulada por diversos psicólogos, bajo la cual la personalidad humana presenta cinco grandes valores. Estos valores son 1) la extroversión o surgencia (*openness to experience*), relacionada con el afecto, asertividad, actividad, búsqueda de emociones y emociones positivas, 2) la agradabilidad o simpatía (*agreeableness*), relacionada con la confianza, honradez, altruismo, cumplimiento, modestia y sensibilidad, 3) la consciencia, conformidad, o seguridad (*conscientiousness*), relacionada con la competencia, orden, obediencia, lucha por el logro, autodisciplina, reflexión, 4) el neuroticismo, inestabilidad emocional o inquietud (*neuroticism*), relacionada con la ansiedad, hostilidad colérica, depresión, timidez, impulsividad, vulnerabilidad, y 5) la apertura a la experiencia (*openness to experience*), relacionada con la fantasía, estética, sentimientos, acciones, ideas, valores. *Vid.* Ter Laak, J., «Las cinco grandes dimensiones de la personalidad», *Revista de Psicología de la PUCP*, vol. xiv, núm. 2, 1996, pp. 138-139.

usuarios de Facebook con mensajes muy específicos[155-156]. Tras la publicación del informe, se produjo un escándalo a nivel global en el que la manipulación política mediante redes sociales se puso en el punto de mira. El escándalo resultó incluso en un documental de Netflix, llamado *El Gran Hackeo*, en el que se relata, conforme al resumen que aporta el propio Netflix, cómo «Cambridge Analytica, empresa experta en el análisis de datos, se convirtió en el lado oscuro de las redes sociales tras las elecciones presidenciales de 2016 en EE.UU.».

Si relacionamos este caso con la especial protección otorgada a los datos sensibles, encontramos la gran problemática de que los datos personales recolectados no eran, individualmente, datos sensibles, sino que es el análisis de estos lo que revela información sensible, como la opinión o tendencia política del individuo. Volvemos, pues, a la problemática de los *proxies*. Ahora bien, si damos por reproducidos los argumentos anteriores relativos a una interpretación funcional de los *proxies*, podemos concluir que éstos, en casos como el de Cambridge Analytica, presentan la naturaleza de datos sensibles, ya que revelan opiniones políticas de sujetos identificados o identificables. Igualmente, el hecho de que los *proxies* se utilicen para manipular las decisiones electorales de los votantes va en contra del espíritu mismo de la protección de los datos sensibles, el cual es la protección de los sujetos de datos frente a inferencias sobre los derechos y libertades fundamentales.

A nivel regulatorio, como veremos en posteriores apartados, la Unión Europea ha querido afrontar el desafío de la manipulación de datos reveladores de opiniones políticas, donde cabe destacar la DSA, así como la propuesta de Reglamento sobre la transparencia y la segmentación de la publicidad política.

2.6. *Datos reveladores de afiliación sindical*

Otra categoría de datos sensibles son los reveladores de afiliación sindical. Si atendemos a la Carta de los Derechos Fundamentales de la UE[157], éstos merecen una protección especial con el fin de salvaguardar la libertad individual de negociación y acción colectiva, así como para impedir la discriminación de las personas en el mercado de trabajo por razón de sus actividades sindicales[158]. Por su parte, el CEDH protege la libertad de reunión y asociación, señalando que toda persona tiene

---

[155] Heawood, J. «Pseudo-public political speech…», *op. cit.*

[156] Hinds, J., Williams, E. J. y Joinson, A. N. «"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal», *International Journal of Human-Computer Studies*, vol. 143, 2020, pp. 1-14.

[157] *Vid.* Art. 28 de la Carta de los Derechos Fundamentales de la UE.

[158] Voigt, P. y Von Dem Bussche, A. *The EU General Data Protection Regulation…, op. cit.,* pp. 92-116.

derecho a la libertad de reunión pacífica y a la libertad de asociación, incluido el derecho a fundar, con otras, sindicatos y de afiliarse a los mismos para la defensa de sus intereses[159]. En España, la CE protege igualmente el derecho fundamental a la libertad sindical[160].

En el ámbito publicitario, sería posible que la publicidad sobre determinadas ofertas —como puestos de trabajo— varíe por la afiliación del destinatario a un sindicato. Así, a título de ejemplo, si la empresa anunciante ve problemático que un potencial trabajador esté afiliado a cualquier sindicato, o a uno concreto con el que la empresa suela tener diferencias, podría procurar que sus anuncios para puestos de trabajo no sean visibles para tales destinatarios, si la plataforma le ofrece dicha opción. Un caso similar, como hemos señalado anteriormente, ocurrió con los anuncios sobre alojamiento en Facebook, que otorgaba la opción a los anunciantes de excluir a destinatarios de ciertas etnias[161].

Si bien estas prácticas podrían ser declaradas discriminatorias, desde la perspectiva de protección de datos nos enfrentamos con el problema de la naturaleza de los *proxies*. Ciertos comportamientos, como dar «me gusta» o compartir una publicación de determinados sindicatos en redes sociales, pueden ser reveladores de una afinidad ideológica del sujeto con el sindicato en cuestión o con determinadas publicaciones y acciones del mismo. Ahora bien, el caso que aquí se nos plantea es distinto a la problemática de los *proxies* reveladores de otras categorías de datos sensibles.

En otros apartados hemos argumentado como idea principal que los *proxies* pueden tener la consideración de datos sensibles si actúan funcionalmente como datos sensibles. Sin embargo, en estos otros casos, la formulación de la norma era bastante amplia, al referirse a datos relativos a salud, datos relativos a convicciones religiosas o filosóficas, o a datos reveladores de opiniones políticas, de la vida sexual o de la orientación sexual. Sin embargo, la formulación de la norma es mucho más cerrada en el caso de los datos reveladores de afiliación sindical. En esta categoría de datos, solo hay dos opciones: que el individuo esté afiliado a un sindicato, o no lo esté. En los demás datos sensibles, hay un mayor margen de interpretación (o de duda), ya que términos como la salud, las convicciones religiosas o filosóficas o las opiniones políticas son evidentemente amplios. La afiliación sindical, al contrario, es una noción mucho más restringida.

Intentar ampliar el contenido del precepto recurriendo a la interpretación puede ser una tarea ardua. Bajo una interpretación literal,

---

[159] *Vid.* Art. 11.1 CEDH.

[160] *Vid.* Art. 28 CE.

[161] Parris, T. y Angwin, J. «Facebook lets advertisers exclude…», *op. cit.*

el precepto se refiere a *afiliación sindical*, que no, por ejemplo, a «afinidad sindical». Igualmente, bajo una interpretación contextual, ni los considerandos ni el articulado del RGPD arrojan más luz sobre este tema. En cuanto a una interpretación teleológica, podría argumentarse que, en la UE, la protección de la libertad sindical no queda restringida a la mera afiliación sindical, sino que se extiende también a la actividad sobre la misma. Así, señala la Carta de Derechos Fundamentales que el objeto de proteger la libertad sindical es salvaguardar la libertad individual de negociación y acción colectiva, así como impedir la discriminación de las personas en el mercado de trabajo por razón de sus actividades sindicales[162]. La necesidad de flexibilizar este término también se ha advertido por parte de las autoridades nacionales de protección de datos, al argumentar que el grado de sensibilidad de los datos sobre afiliación sindical puede variar en función del país en el que nos encontremos[163].

Sin embargo, esta visión amplia no es compatible con la formulación literal de la norma. También se aparta de ella la AEPD, mostrando una perspectiva más limitada a la hora de interpretar los datos de afiliación[164]. A título de ejemplo, en una de sus resoluciones, la Agencia señaló que la pertenencia a órganos de representación unitaria en la empresa no presupone la afiliación. En el caso en concreto, se compartió en Internet una lista donde se presentaba al trabajador como perteneciente a un órgano de representación unitaria en la empresa, pero la Agencia entendió que de este dato no se infiere que el denunciante estuviese afiliado al sindicato CC. OO., por lo que tenía la consideración de dato personal básico y no de dato sensible[165].

Ante esta visión reduccionista de la norma planteamos dos opciones. La opción *de lege ferenda* sería una modificación de la literalidad del RGPD, incluyendo el tratamiento de datos que revelen «la afiliación, afinidad o actividad sindical» del sujeto de datos. A nuestro entender, la segunda opción, *de lege lata,* sería interpretar que los *proxies* relacionados con una actividad o afinidad sindical son datos reveladores de opiniones políticas. El concepto de opiniones políticas es un concepto bastante amplio, en el que sin duda pueden tener cabida las ideologías sobre derechos de los trabajadores, por lo que la categoría de datos reveladores de opiniones políticas podría englobar aquellos datos que no revelen la afiliación sindical del sujeto de datos,

---

[162] Voigt, P. y Von Dem Bussche, A. *The EU General Data Protection Regulation…, op. cit.,* pp. 92-116.

[163] Article 29 Data Protection Working Party, «Advice paper on special categories…», *op. cit.*

[164] Gualda Alcalá, F. J. «Los datos que revelen la afiliación sindical como categoría especial de datos personales (comentario al art. 9.1. RGPD)», en Troncoso Reigada, A. *Comentarios al Reglamento General…, op. cit.,* pp. 1095-1108.

[165] Resolución 1029/2009, de 17 de abril de la AEPD.

pero que, sin embargo, estén relacionados con sus actividades o afinidades sindicales.

2.7. *Datos relativos a convicciones religiosas o filosóficas*

El RGPD incluye como datos especialmente protegidos los relativos a las convicciones religiosas o filosóficas. La libertad religiosa está protegida a nivel internacional por el art. 10 de la Carta de Derechos Fundamentales de la UE[166], así como por el art. 9 del CEDH[167]. Igualmente, la no discriminación por motivos de religión también es protegida por el CEDH[168] y por la Carta[169], esta última reconociendo también el derecho a la diversidad religiosa[170].

El RGPD no llega a ofrecer una definición del término *convicciones religiosas o filosóficas*, ni en su articulado ni en sus considerandos. Esta omisión tiene sentido, ya que la libertad religiosa es un tema particularmente sensible y variable dependiendo del contexto nacional en el que nos encontremos, y en el que la doctrina y tradiciones religiosas de cada país y comunidad juegan un papel importante.

Sin ánimo de recrearnos en amplios debates doctrinales, nos centraremos en qué datos pueden ser considerados como reveladores de esta categoría, ya que, en la práctica, las orientaciones del último siglo de derecho eclesiástico, jurisprudencia y doctrina se inclinan por un tratamiento equiparado de las creencias religiosas y de las convicciones no religiosas (que podrían englobarse bajo la calificación de *filosóficas*)[171].

Entre los datos reveladores de convicciones religiosas o filosóficas, ciertos autores señalan que se debe incluir aquella información que permita sacar conclusiones sobre la afiliación religiosa de una persona, o sobre la falta de ella, así como la práctica de la religión[172]. Por su parte, otros autores sostienen que en este concepto deben tener cabida no solo los datos de la pertenencia a una confesión religiosa, sino también de pertenencia a una organización que se centre en una creencia filosófica.

---

166 *Vid.* Art.10 de la Carta.

167 *Vid.* Art. 9 CEDH.

168 *Vid.* Art. 14 CEDH.

169 *Vid.* Art. 21.1 de la Carta.

170 *Vid.* Art. 22 de la Carta.

171 *Vid.* Por todos, Martínes-Torrón, J. «La protección internacional de la libertad religiosa y de conciencia, cincuenta años después», *Revista de la Facultad de Derecho de la Universidad de Granada*, 1999, pp. 63-88.

172 Voigt, P. y Von Dem Bussche, A. *The EU General Data Protection Regulation…, op. cit.,* pp. 92-116.

A nuestro entender, la inclusión de esta categoría de datos como datos sensibles plantea numerosos problemas interpretativos. El principal problema es el concepto mismo de convicciones filosóficas. La declaración de pertenencia a organizaciones filosóficas y no confesionales, si bien revela las convicciones filosóficas, es mucho más imprecisa que una declaración de pertenencia a una religión. En las organizaciones filosóficas no confesionales no se dan relaciones jurídicas estrictamente diferenciadas, en contraste a otras asociaciones o agrupaciones humanas[173]. En este extremo, en nuestra opinión, radica la razón de que la doctrina tienda a obviar la parte relativa a la filosofía y se centre en los datos reveladores de convicciones religiosas, al resultar evidente que las convicciones religiosas tienen una estructura social mucho más marcada que las convicciones filosóficas.

Esta dificultad ya era evidente en 2011, cuando el Grupo de Trabajo del Artículo 29 elaboró una serie de recomendaciones sobre datos sensibles, en las cuales instaba a optar por un término más preciso que «datos reveladores de convicciones religiosas», ya que este era difícil de definir, dando lugar a divergencias esperpénticas como, por ejemplo, que un tribunal de Reino Unido considerase la creencia en el cambio climático como un dato sensible, al ser revelador de una convicción filosófica[174]. Esta recomendación, como resulta patente, no llegó a dar resultados fructíferos ante la dificultad de encontrar una formulación alternativa que aunase datos con connotaciones éticas o morales, como la objeción de conciencia, el rechazo al aborto o a la eutanasia.

Podría señalarse, igualmente, que datos como los anteriores, de un carácter ideológico controvertido, ya suelen quedar amparados por otras categorías especiales de datos, como los reveladores de opiniones políticas. El trasfondo de estas categorías de datos es, en términos generales, proteger los derechos y libertades fundamentales, evitando la discriminación con base a las ideologías diversas que pueda guardar el sujeto de datos, por lo que en la práctica, una gran cantidad de datos ideológicos pueden tener cabida en el concepto de datos sensibles, si bien esta amplitud presenta el doble filo de ser una obligación legal excesivamente difícil de asumir por las entidades que manejan cantidades masivas de datos.

Por otro lado, la formulación del término «datos que revelen convicciones religiosas» resulta igualmente problemática, ya que no se precisa el alcance del término *revelar*. Podría entenderse que se hace referencia a una simple apariencia, es decir, a datos personales en los que se pueda presumir o inferir una determinada creencia o convicción. Pero esta consideración no deja de ser una deducción a partir de datos

---

[173] González Moreno, B. «Los datos que revelen…», *op. cit.*

[174] Article 29 Data Protection Working Party, «Advice paper on special categories…», *op. cit.*

o *proxies* que parecen indicar unas convicciones, lo que es sustancialmente diferente del dato objetivo de pertenencia o adscripción a una confesión religiosa o a una organización confesional[175].

En otras palabras, podríamos afirmar que existen datos distintos a las declaraciones de pertenencia, como usar un determinado tipo de pañuelo sobre la cabeza, vestir un atuendo religioso, portar una cruz católica o negarse a consumir determinados alimentos, que pueden constituir *proxies* susceptibles de revelar la creencia religiosa del individuo, pero no necesariamente manifiestan la creencia religiosa del individuo. Dependiendo del tipo de *proxy*, puede derivarse la convicción religiosa bien con el *proxy* en cuestión de forma individual, o bien de forma inferida, en combinación con otra serie de datos. Un ejemplo del primer caso sería portar un hábito religioso, como una sotana. Del mismo puede deducirse individualmente la posible pertenencia del individuo a la religión católica. En cambio, un ejemplo del segundo caso sería que una persona no consuma productos derivados del cerdo. Aisladamente, este *proxy* puede significar que es musulmana, pero también puede significar muchas otras cosas, como ser vegetariana, vegana, o que simplemente no le agraden estos productos. Ahora bien, si el algoritmo detecta este *proxy* junto con muchos otros, como el portar un hiyab y acceder frecuentemente a contenidos sobre el Corán, el margen de acierto sobre la creencia religiosa será mucho mayor.

En el marco de las apps digitales, la presencia de datos indicadores de convicciones religiosas también ha ido ganando un mayor protagonismo. La búsqueda y acceso a determinadas páginas web puede revelar la convicción religiosa del individuo, aunque se plantea el dilema de si, por ejemplo, el mero acceso a una página web con análisis de versículos de la Biblia ya es un dato sensible, o si es la suma de este dato con muchos otros la que otorga la información sensible. Por otro lado, ciertas conductas, como suscribirse a una newsletter sobre eventos de una determinada religión, o descargar una app de oraciones católicas como Hallow, pueden ser reveladoras, aisladamente, de la convicción religiosa del usuario.

Sea de forma aislada o de forma inferida, en la práctica el análisis de estos *proxies* debería ser considerado un tratamiento de datos sensibles, cuando presente la capacidad o el propósito de revelar la convicción religiosa del individuo y surja, en consecuencia, un riesgo de discriminación o de producción de otros efectos adversos con base a esta convicción religiosa. Esta justificación obedece a la interpretación funcional que hemos aplicado previamente a las demás categorías de datos sensibles y que damos aquí por reproducida.

---

[175] González Moreno, B. «Los datos que revelen…», *op. cit.*

2.8. *Datos relativos a la vida sexual u orientación sexual*

La última categoría de datos sensibles incluida en el RGPD son los datos relativos a la vida u orientación sexual de una persona física, datos cuya protección tiene amplio reconocimiento a nivel internacional. La protección de la vida sexual conforma una parte del derecho a la vida privada y familiar bajo la Carta de Derechos Fundamentales[176] y el CEDH[177]. La Carta[178], en coherencia con el TFUE[179], también protege frente a la discriminación por orientación sexual.

Como señalan algunos autores, las categorías «datos relativos a la vida sexual» y «datos relativos a la orientación sexual» están intrínsecamente conectadas, pero no son idénticas[180]. La orientación sexual se refiere a información que comprende, por ejemplo, si un individuo es heterosexual, homosexual, bisexual u otra orientación[181]. Los datos relativos a la vida sexual pueden incluir no solo el anterior aspecto, sino también información sobre prácticas sexuales (como el consumo de pornografía), así como detalles maritales y aspectos íntimos (como el cambio de género o el uso de anticonceptivos)[182]. Señalan algunos autores, por otro lado, que la repercusión en la vida del afectado podría ser diferente, ya que la revelación de la identidad sexual puede resultar especialmente estigmatizante en ciertos contextos demográficos[183].

Respecto a los datos reveladores de la vida sexual, resulta evidente que la presencia digital de los mismos ha crecido exponencialmente en los últimos años. Este crecimiento se manifiesta en el número de usuarios que acceden a plataformas con contenido pornográfico. Un ejemplo claro es que la Comisión Europea decidiese incluir a tres de estas plataformas —PornHub, Stripchat, y Xvideos— en la lista de plataformas de muy gran tamaño en aplicación de la DSA[184]. Traducida en números, dicha designación significa que cada una de estas plataformas de contenido pornográfico tiene un promedio mensual de, al menos, 45 millones de usuarios activos en la UE. Los riesgos derivados del acceso a estas plataformas no son escasos. Si bien una de las preocupaciones principales es el acceso a estas plataformas por menores de edad, también se dan riesgos relevantes para usuarios que no

---

[176] *Vid.* Art. 7 de la Carta.
[177] *Vid.* Art. 8 CEDH.
[178] *Vid.* Art. 21.1 de la Carta.
[179] *Vid.* Art. 10 TFUE.
[180] Ludmila, G. y Kuner, C. «Article 9 Processing of special…», *op. cit.*
[181] *Ibid.*
[182] *Ibid.*
[183] Gómez Sánchez, Y., «Categorías especiales de datos personales…», *op. cit.*
[184] European Commission Press Corner, «Commission designates second set of Very Large Online Platforms under the Digital Services Act», 2023.

son menores. Entre ellos destaca el hecho de que los datos sensibles recolectados por la plataforma puedan ser utilizados para la construcción de un perfil del usuario con fines variados y de los que puedan derivar consecuencias adversas.

La lista de datos reveladores de la vida sexual y de la orientación sexual que pueden obtenerse en el entorno digital es amplia. El acceso y búsqueda de páginas web con contenido pornográfico, la compra y búsqueda *online* de productos anticonceptivos o productos sexuales o los clics efectuados sobre anuncios relativos a estos productos revelan datos sobre la vida sexual de un individuo. Las *apps* de citas, por ejemplo, son una fuente inagotable de datos sensibles. Las declaraciones que hace el usuario en su perfil revelan su orientación sexual e incluso, en ocasiones, sus preferencias relativas a la vida sexual. A modo de ejemplo, Tinder ofrece actualmente al usuario la posibilidad de elegir entre nueve orientaciones sexuales: heterosexual, gay, lesbiana, bisexual, asexual, demisexual, pansexual, queer y «tengo dudas».

El mero hecho de descargar una aplicación de citas como Grindr, sin siquiera llegar a usar la aplicación, revela la pertenencia o afinidad del usuario con el colectivo LGTBQ. La magnitud del número de datos sensibles recolectados por Grindr es apabullante. La propia página web de Grindr describe su servicio como «la aplicación de red social más grande para personas homosexuales, bisexuales, trans y queer». Su página web afirma que tienen millones de usuarios diarios, y que «utilizan su tecnología basada en la ubicación en casi todos los países y en todos los rincones del planeta». Igualmente, el historial que guarda la plataforma sobre cuántas citas tiene el usuario revela datos sobre la vida sexual del individuo.

Este fenómeno también ocurre en las redes sociales. En Facebook, por ejemplo, muchos usuarios indican en su perfil la identidad de su pareja, idea poco recomendable en términos de privacidad, ya que puede revelar tanto la vida sexual como la orientación sexual del individuo. La problemática del uso de *proxies* tampoco es ajena en esta categoría de datos. Algunos autores señalan desde hace años que el algoritmo de Facebook puede inferir la orientación sexual del usuario (y otras características sensibles) a partir de las interacciones de este en la plataforma[185]. Así, por ejemplo, hay estudios que muestran cómo los *likes* de Facebook pueden utilizarse para predecir de forma automática y precisa características sensibles como «la orientación sexual, la etnia, las opiniones religiosas y políticas, los rasgos de personalidad,

[185] González Cabañas, J., Cuevas, A. y Cuevas, R. «Facebook use of sensitive data for advertising in Europe», *27th USENIX Security Symposium*, 2018, pp. 479-495.

la inteligencia, la felicidad, el consumo de sustancias adictivas, la separación de los padres, la edad y el sexo»[186].

Uno de estos estudios se basó en un conjunto de datos de más de 58 000 voluntarios, quienes proporcionaron tanto sus *likes* de Facebook como sus perfiles demográficos detallados y los resultados de varias pruebas psicométricas[187]. El modelo discriminó correctamente entre hombres homosexuales y heterosexuales en el 88 por ciento de los casos, entre afroamericanos y caucásicos en el 95 por ciento de los casos, y entre demócratas y republicanos en el 85 por ciento de los casos. Este estudio, entre muchos otros, revela la increíble precisión con la que el algoritmo infiere una gran cantidad de conclusiones y datos sensibles sobre los usuarios a través de *proxies*, y nos lleva a plantearnos, lógicamente, los usos nocivos que pueden llevarse a cabo con dichos conocimientos.

Igualmente, se plantea la disyuntiva de si es conveniente aplicar una interpretación funcional a este tipo de *proxies*. Muchos de los *proxies* utilizados para perfilar la orientación sexual o la vida sexual de un individuo son, de forma aislada, muy distantes y ajenos a la orientación sexual o la vida sexual. Así, el algoritmo puede usar como *proxy* para determinar la orientación sexual tener un determinado automóvil, pero este dato, de forma aislada, poco o nada tiene que ver con la orientación sexual, sino que es la combinación de este dato con muchos otros la que puede llevar a deducir el dato sensible. Si llevásemos a cabo una interpretación excesivamente funcional, teniendo en cuenta la cantidad masiva de datos que se pueden combinar para llegar a conclusiones sensibles, casi todos los datos personales podrían tener la naturaleza de sensibles, lo que generaría una cascada de problemas que serán objeto de consideración a continuación.

IV. ¿DEVALUACIÓN DEL CONCEPTO «DATOS PERSONALES SENSIBLES» BAJO UNA INTERPRETACIÓN FUNCIONAL? LA SENSIBILIDAD POR DISTANCIA COMO CONTRAPESO

Anteriormente, planteábamos la necesidad de extender la interpretación del concepto mismo de datos sensibles de forma que integre a los datos inferidos y a los *proxies*. Proponíamos una interpretación funcional, en virtud de la cual, si los datos inferidos o los *proxies* sir-

[186] Kosinski, M., Stillwell, D. y Graepel, T. «Private traits and attributes are predictable from digital records of human behavior», *Proceedings of the National Academy of Sciences (PNAS)*, 2013, pp. 5802-5805.

[187] González Cabañas, J., Cuevas, A. y Cuevas, R. «Facebook use of sensitive…», *op. cit.*

ven para concluir o sustituir datos sensibles, deben presentar el mismo tratamiento legal que éstos ya que, como señalan algunos autores, «los datos son lo que los datos hacen»[188].

Ahora bien, es necesario tener en cuenta que la interpretación funcional puede presentar la desventaja de abocar a una inflación indeseada del concepto. En la era del *Big data* y de la IA, cualquier dato personal puede potencialmente llegar a ser utilizado para concluir datos sensibles. Algunos autores señalan que esta inflación podría resultar en una depreciación de la regulación sobre el tratamiento de datos sensibles, ya que todos los datos personales, funcionalmente, podrían ser datos sensibles si son combinados algorítmicamente con otra serie de datos[189][190].

Esta inflación del concepto de datos sensibles podría moderarse hasta cierto punto si consideramos la distancia que media entre los datos analizados (*prima facie* no sensibles) y los datos o inferencias que sí son sensibles conforme a la normativa de protección de datos. Siguiendo este análisis, resolveríamos el problema práctico de que las inferencias sensibles no se plasmen en ningún punto del proceso algorítmico, ya que el punto de referencia para el análisis de sensibilidad sería el dato indicador o *proxy* que da lugar a una respuesta automática por parte del algoritmo, sin necesidad de que se cree un dato nuevo[191]. En otras palabras, el examen se enfocaría en los datos personales tenidos en cuenta para que se aplique una determinada respuesta, o, en el ámbito que aquí planteamos, en los datos personales considerados para seleccionar los destinatarios, personalizar el contenido del anuncio o excluir a determinados individuos de ciertos anuncios.

---

[188] Solove, D. J. «Data is what data does; regulating based on harm and risk instead of sensitive data», *Northwestern University Law Review*, vol. 118, núm. 4, 2024.

[189] Por todos, *vid.* Malgieri, G. y Quinn, P. «The Difficulty of Defining…», *op. cit.*

[190] Conviene añadir que el único problema podría no ser la depreciación del concepto, sino que, por otro lado, los responsables de tratamiento podrían verse sometidos a cargas excesivas. Si una gran cantidad de *proxies* y datos inferidos pasan a tener la consideración de datos sensibles, los responsables deberán cumplir con una serie de obligaciones adicionales. A título de ejemplo, aparte de cumplir con las bases de tratamiento aplicables a los datos sensibles, si llevan a cabo un tratamiento de datos sensibles «a gran escala» (lo cual será frecuente si atendemos a una interpretación funcional), deberán designar a un delegado de protección de datos y llevar a cabo una evaluación de impacto, por no mencionar que el RGPD habilita a los Estados Miembros para mantener o introducir garantías adicionales para el tratamiento de datos genéticos, biométricos o relativos a la salud.

[191] Entendiendo en este caso «nuevo» como un dato inferido a partir de datos que sí han sido generados por el usuario. Atendiendo a su generación, hay autores que distinguen entre datos en bruto o datos generados por los usuarios, por un lado, y datos complejos o datos generados por el responsable del tratamiento, por otro lado. En esta categorización, los datos nuevos o datos inferidos caerían bajo la categoría de datos complejos o datos generados por el responsable de datos. Para una explicación más detallada de estas categorías, *vid.* Malgieri, G. y Comandé, G. «Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era», *Information, Communication and Technology Law*, núm. 3, 2017, pp. 4.

Poniendo un ejemplo, ciertos estudios muestran que el código postal, frecuentemente, puede ser un indicador bastante exacto de la raza del individuo[192]. Si el algoritmo publicitario es entrenado para excluir a determinados destinatarios que presenten un código postal concreto, el anunciante podría argumentar que en ningún momento el algoritmo tiene en cuenta datos sensibles como la raza. Sin embargo, a efectos prácticos, se puede estar utilizando el código postal como dato sustitutivo de la raza del individuo con fines discriminatorios. En casos como este, analizar la sensibilidad por distancia sería útil para determinar cómo de cerca está el código postal de inferir la raza en cada caso particular, si bien el análisis deberá realizarse casuísticamente, ya que la distancia computacional puede variar en ejemplos como el presentado.

A este análisis de sensibilidad se le denomina ya por ciertos autores como *sensibilidad de los datos por distancia computacional*, o de forma más abreviada, *sensibilidad por distancia*[193]. Este análisis tiene en cuenta dos variables: *a)* la *sensibilidad intrínseca* de los datos y *b)* cómo de alejados están estos datos (*prima facie* no sensibles) de inferencias que sí son sensibles. Este último factor es lo que se conoce como *distancia computacional*.

El primer factor, la sensibilidad intrínseca, está fuertemente anclado a las limitaciones que predominan en el texto del RGPD, y depende en gran medida de la interpretación que realizamos sobre el concepto de datos sensibles. Si bien el Grupo de Trabajo del Artículo 29 (actualmente CEPD) y el TJUE han ido abriendo paso a unas interpretaciones más amplias del concepto de datos sensibles, la sensibilidad intrínseca continúa siendo un concepto enormemente abstracto y sujeto a muchas inseguridades jurídicas que se plasman en la práctica. Algunos ejemplos de estas inseguridades son los denominados «datos cuasi-sensibles», es decir, datos cuya sensibilidad no resulta del todo clara. En la categoría de datos relativos a la salud, algunos ejemplos de datos cuasi-sensibles serían los datos sobre la dieta diaria, los pasos andados, o algunas inferencias como la esperanza de vida[194].

Debido a tal inseguridad jurídica, diversos autores, ofreciendo una opinión que compartimos, sostienen la necesidad de complementar la sensibilidad intrínseca con otros factores. En el caso que anteriormente planteábamos, es posible que el código postal, de forma genérica y sin tener en cuenta el contexto, tenga un carácter sensible dudoso. Es decir, no todos los códigos postales serán datos reveladores de la raza, sino que dependerá del código postal en cuestión e, igualmente, aunque se trate de un código postal en el que habite un gran porcentaje de minorías raciales, puede que no siempre se utilice con fines

[192] Calabresi, G. «Ideals, Beliefs, Attitudes,…», *op. cit.,* pp. 35-36.
[193] Malgieri, G. y Comandé, G. «Sensitive-By-Distance…», *op. cit.*
[194] *Ibid.*

discriminatorios. El examen, por tanto, habrá de ser casuístico, ya que la distancia entre el código postal y los datos sobre el origen étnico o la raza puede diferir según diferentes contextos y medios disponibles. A este segundo factor se le denomina distancia computacional, la cual requiere medir el nivel de esfuerzo y distancia para inferir datos sensibles de otros que aparentemente no lo son[195].

La principal ventaja de la distancia computacional, a nuestro entender, sería paliar la inflación excesiva del concepto que puede derivar de una interpretación funcional. Planteábamos anteriormente que, conforme al actual estado de la técnica, cualquier dato podría ser potencialmente un dato sensible si es combinado con otros datos disponibles. Sin embargo, esta aproximación podría llevar a una depreciación del concepto y a excesivas cargas para los responsables de datos. Si moderamos esta aproximación con la distancia computacional, solo aquellos datos en los que medie una distancia corta con datos puramente sensibles caerían dentro de esta última categoría.

La distancia computacional podría medirse bajo una perspectiva objetiva o subjetiva. Bajo la perspectiva objetiva, la distancia computacional depende de tres variables que se aplican a todos los responsables de datos por igual, razón por la cual es calificada como «perspectiva objetiva». Estas variables pueden ser:

— El nivel de desarrollo de las tecnologías de minería de datos disponibles en cada momento a un coste razonable.
— La disponibilidad de datos adicionales o accesorios, ya sean personales o no personales.
— La concurrencia de restricciones al tratamiento de datos, debido a cualquier tipo de obligación de confidencialidad. En particular, es frecuente que los datos inferidos estén protegidos por secreto empresarial, lo cual puede resultar un obstáculo para su transferencia, tanto hacia otras empresas como para los sujetos de datos, teniendo también en cuenta que sobre los datos inferidos no rige el derecho a la portabilidad[196].

Estas tres variables se corresponden con tres de las cuatro fuerzas que, según Lawrence Lessig, regulan la vida de los individuos, y que son, respectivamente: la arquitectura (entendida como infraestructura técnica del momento), los datos del mercado y la Ley[197].

Trasladando esta teoría al análisis de la distancia computacional, podríamos decir que no todos los datos deben ser considerados sensibles, sino que solo merecen tal calificación aquellos que, conforme

[195] *Ibid.*
[196] *Ibid.*
[197] Lessig, L. *Code 2.0*, CreateSpace Independent Publishing Platform, 2009, p. 123.

al estado de la técnica, permitan inferir de forma razonable conclusiones sensibles —fuerza de la *arquitectura*—, conforme a los datos accesibles en el mercado —fuerza de *los datos*—, y teniendo en cuenta posibles restricciones o limitaciones legales en cuanto a su acceso —la fuerza de la *ley*. Como es evidente, estas fuerzas, en el caso de la distancia computacional, son interdependientes, ya que el avance del estado de la técnica depende enormemente de los datos de entrada —tomemos como ejemplo el entrenamiento de IA con datos-, y la Ley, en su vertiente restrictiva, puede funcionar también como un freno a la transferencia de datos y a la innovación científica.

Por otra parte, la distancia computacional puede abordarse también desde una perspectiva subjetiva. Ésta tiene en cuenta los recursos de que dispone una empresa individualmente considerada para inferir datos sensibles, en lugar de utilizar con carácter general factores genéricos válidos para todas las entidades. El examen individualizado de estos recursos es la causa de que esta perspectiva sea denominada por algunos autores como «perspectiva subjetiva», pudiendo ser los recursos a examinar de diversa índole, como financieros, humanos, o datos previamente adquiridos por la propia entidad.

A nuestro juicio, sería necesario integrar ambas perspectivas, la objetiva y la subjetiva. A menudo se critica que el RGPD sea una norma de «talla única», al resultar de aplicación a todas las entidades, sin distinguir entre el tamaño de los responsables o la industria a la que pertenecen[198]. Esta falta de distinción se vería remediada hasta cierto punto con la inclusión de una perspectiva subjetiva, ya que la probabilidad de que se infieran datos sensibles será más alta para aquellas entidades con mayores recursos, especialmente las *Big Tech*.

Ahora bien, en la práctica, la propuesta de medir la sensibilidad por distancia necesitará de mecanismos jurídicos y técnicos que aseguren su implementación. Problemática se plantea la transparencia de los parámetros utilizados por los algoritmos y las instrucciones dadas a los mismos para que se llegue a una decisión y no a otra. Sin acceso a estos parámetros, no será posible auditar la distancia entre los datos utilizados y las inferencias sensibles. Al mismo tiempo, pueden darse situaciones en las que la trazabilidad de los datos inferidos en el sistema de IA sea posible pero los datos estén protegidos como secretos empresariales[199]. La transparencia en el caso del uso de datos sensi-

---

[198] Ebers, M. y Sein, K., «Data-driven Technologies…, *op. cit.,* pp. 16-23.

[199] Para un análisis detallado sobre las tensiones entre la protección de datos y los secretos empresariales, *vid.* Noto La Diega, G. «Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information», *JIPITEC*, 2018; y Wachter, S. «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbian Business Law Review,* 2019.

bles con fines publicitarios se plantea como una complicada cuestión que trataremos más adelante.

Por último, cabe destacar que, aun en el mejor de los escenarios, si se consigue integrar una interpretación funcional moderada con la distancia computacional como contrapeso, la remisión por parte de la DSA al concepto de datos sensibles del RGPD presenta una tara que no debemos pasar por alto. Como comentábamos en apartados anteriores, la lista de datos sensibles del art. 9 del RGPD es una lista *numerus clausus*. Si bien algunos datos pueden tener el carácter de cuasi-sensibles, como el número de pasos andados o los hábitos alimenticios respecto a los datos relativos a la salud, los mismos guardan una cierta relación con alguno de los datos personales reconocidos en la lista. Sin embargo, hay otros datos personales cuyo encaje en el art. 9 RGPD es mucho más complicado, al no guardar relación clara con ninguna de las categorías especiales referidas en el mismo.

V. DATOS PERSONALES NO INCLUIDOS EN LA LISTA DE DATOS SENSIBLES DEL RGPD

La problemática que supone la remisión al concepto de datos sensibles en la prohibición de la DSA puede desdoblarse en dos partes. La primera, expuesta en apartados anteriores, es la dificultad para determinar qué datos personales son sensibles, sobre todo en aquellos casos en los que se utilizan *proxies* para sustituir a los mismos o se infieren nuevos datos sensibles sin que tengan una trazabilidad clara en el sistema de IA, en particular cuando los datos en cuestión son protegidos como secretos empresariales[200]. Al mismo tiempo, una interpretación excesivamente funcional puede dar lugar a que todos los datos personales sean potencialmente datos sensibles, lo cual desvirtuaría su regulación especial en la denominada era de las inferencias o era del *Big data*[201]. Aun si intentásemos moderar el nivel de datos que pueden constituir datos sensibles aplicando la sensibilidad por distancia propuesta por Malgieri y Quinn, seguiríamos enfrentándonos a la problemática de que la distancia computacional debe medirse en referencia a una de las categorías de datos sensibles incluidas en el art. 9.1 del RGPD[202].

Esta limitación nos lleva a apuntar la segunda parte de la problemática: los datos no incluidos en la lista de datos sensibles. Como exponíamos en otro lugar, la *raison d'être* de establecer una regulación específica sobre los datos sensibles no es otra que la protección de los

[200] Noto La Diega, G. «Against the Dehumanisation of Decision-Making…», *op. cit.*
[201] Solove, D. J. «Data is what data does…», *op. cit.*
[202] Malgieri, G. y Quinn, P. «The Difficulty of Defining…», *op. cit.*

individuos frente a posibles efectos adversos derivados del uso de tales datos. Entre estos potenciales riesgos adversos destaca la puesta en peligro de los derechos y libertades de los individuos, lo que incluye la no discriminación, pero también, de forma más particular, posibles daños físicos, psíquicos, sociales o económicos[203]. Estos efectos, como desarrollaremos más adelante, pueden tener un protagonismo especial en ciertas prácticas personalizadas.

En términos generales, los datos no acogidos en el concepto de datos sensibles que pueden dar lugar a consecuencias adversas a través de la publicidad basada en perfiles son innumerables y dependientes de un análisis casuístico, si bien conviene detenernos en algunos ejemplos contextuales para evidenciar la gran problemática que supone la remisión a la lista cerrada de datos sensibles, problemática que también ha sido advertida por un reciente estudio de la Comisión Europea sobre la adecuación de la actual normativa de consumo (en adelante, *Fitness Check 2024*)[204].

La primera categoría cuya exclusión generó fuertes críticas fue el género del sujeto de datos. Durante el proceso legislativo de aprobación del RGPD, diversos grupos parlamentarios propusieron que el género se calificase como un dato sensible, si bien finalmente no se incluyó en la lista y ni siquiera llegó a ser una categoría propuesta por el GT29[205]. Sin embargo, su potencialidad para generar efectos discriminatorios es más que evidente. Algunos estudios sugieren que los algoritmos tienden a favorecer a los hombres sobre las mujeres para las ofertas de empleos STEM en plataformas como Facebook, Google, Instagram y Twitter[206]. Este favorecimiento no siempre es intencionado por parte de la plataforma, es decir, la causa no tiene por qué radicar necesariamente en las instrucciones expresas aportadas al algoritmo, sino en lo que se denomina *preferencias sesgadas*[207]. Si los *inputs* muestran que para los trabajos STEM la mayoría de los trabajadores son hombres, el algoritmo dirigirá las ofertas a los hombres, al derivar que es un dato revelador de los mejores candidatos para la empresa.

Otro caso que no queda claro en la normativa actual es si la identidad de género es un dato sensible. Atendiendo a la literalidad de la norma, la respuesta inicial sería que no, ya que la lista del art. 9.1 del RGPD es una lista cerrada como bien han aclarado el GT29 y la

---

[203] Voigt, P. y Von Dem Bussche, A., *The EU General Data Protection Regulation…, op. cit.,* pp. 92-116.

[204] Entre los ejemplos de datos cuyos usos pueden perjudicar los intereses de los consumidores el estudio cita la situación financiera, el historial de ludopatía o un estado de ánimo negativo. Whittle, M. *et al.*, *Study to support the Fitness Check…, op. cit.,* p. 65.

[205] Article 29 Data Protection Working Party, «Advice paper on special categories…», *op. cit.*

[206] Celis, E., Mehrotra, A. y Vishnoi, N. «Toward Controlling Discrimination…», *op. cit.*

[207] Zuiderveen, B. «Discrimination, artificial intelligence…», *op. cit.*

AEPD[208]. Como señala la OMS, la identidad de género es distinta a la orientación sexual o a la vida sexual, al referirse aquella a «la experiencia de género interna, individual y profundamente sentida de una persona, que puede corresponderse o no con la fisiología de la persona o el sexo designado al nacer»[209]. En el mismo sentido se pronuncia el art. 2(1) de la Ley 2/2021, de 7 de junio, de igualdad social y no discriminación por razón de identidad de género, expresión de género y características sexuales, al definirla como «la vivencia interna e individual del género tal y como cada persona la siente y autodetermina, sin que deba ser definida por terceros, pudiendo corresponder o no con el sexo asignado al nacer y pudiendo involucrar o no la modificación de la apariencia o de las funciones corporales a través de medios farmacológicos, quirúrgicos o de cualquier otra índole, siempre que ello sea libremente escogido».

Pese a que la identidad de género no es una categoría incluida en la lista *numerus clausus* del art. 9 (1) del RGPD, en España encontramos dos resoluciones de la AEPD que tratan la identidad de género como un dato sensible. En la primera resolución, de 2020, la AEPD sanciona al Departamento de Educación del Gobierno de Navarra por incluir la casilla «otras opciones», en el campo sobre sexo en una encuesta no anónima realizada a estudiantes[210]. La AEPD entiende que los interesados revelarían datos concernientes a su identidad de género, cuestión que, a criterio de la Agencia, puede considerarse «relacionada con la categoría especial de datos sensibles referentes a la orientación sexual». En otra resolución de 2024, la AEPD apercibió a la Consejería de Economía, Conocimiento y Empleo del Gobierno de Canarias por incluir la opción «no binario», en un formulario relacionado con la conciliación previa en conflictos laborales individuales[211]. La AEPD consideró que esta opción podría revelar datos sensibles sobre la orientación o la vida sexual de las personas.

La justificación de las anteriores resoluciones es cuanto menos confusa. Por un lado, en la primera relaciona la identidad de género con la orientación sexual, términos que, como señalábamos, son distintos. En la segunda resolución indica que la identidad de género está relacionada con la orientación sexual o la vida sexual, añadiendo la posibilidad de que esté relacionada con dos categorías diferentes de datos sensibles sin ofrecer argumentos que sostengan esta afirmación. Paradójicamente, la Agencia reconoce que ninguno de estos términos

---

[208] *Vid.* Article 29 Data Protection Working Party, «Advice paper on special categories…», *op. cit.*; y Consulta Número 054388/2019 de la AEPD, p.9. En el mismo sentido se pronuncia la doctrina, por todos, *vid.* Malgieri, G. y Quinn, P. «The Difficulty of Defining…», *op. cit.*

[209] World Health Organization, «Gender and Health».

[210] AEPD, Procedimiento núm. PS/00245/2019.

[211] AEPD, Procedimiento PS/00070/2023.

(identidad de género, orientación sexual y vida sexual) son sinónimos, al mismo tiempo que sostiene que la identidad de género debe interpretarse como un dato sensible ya que la regulación de los mismos tiene como objeto evitar situaciones discriminatorias[212].

Aunque la AEPD pretenda justificar que la identidad de género es un dato *relacionado* con la vida sexual o la orientación sexual, el reconocimiento de que estos términos son distintos es un factor esencial para afirmar que, *de facto,* la AEPD está añadiendo una categoría nueva a la lista de datos sensibles. También es reseñable que ambas decisiones de la AEPD parecen contradecirse con declaraciones previas de la misma AEPD, en las que reconocía a la lista de datos sensibles como una lista *numerus clausus*. En la consulta en cuestión, la Agencia rechazó considerar la condición de víctima de violencia de género como una categoría especial del art. 9 (1) RGPD, sí remitiéndose en este caso, en cambio, a la posibilidad de otorgar una elevada protección a dichos datos a través de otras vías[213].

Por mucho que nos encontremos de acuerdo con la afirmación de que datos como la identidad de género pueden dar lugar a efectos discriminatorios, no podemos ignorar que la extensión de una lista establecida como cerrada en un Reglamento de la UE va en contra de las competencias de una autoridad nacional, vulnerando el sistema de competencias de la UE. Al regular las categorías especiales de datos personales, la UE está legislando en el ámbito de sus competencias en virtud del art. 16 (2) del TFUE[214]. Se podría argumentar en este sentido que la autoridad nacional estaría vulnerando el principio de *pre-emption* o desplazamiento al añadir una nueva categoría a una lista que es exhaustiva salvo expresa autorización, si bien este extremo sale del objeto del presente trabajo[215].

---

[212] AEPD, Procedimiento núm. PS/00245/2019, p. 31.

[213] En la consulta Número 054388/2019 de la AEPD, la misma señaló que «las categorías especiales de datos se han de considerar *numerus clausus*, pues conforman un régimen especial de protección que supone una excepción que limita y circunscribe a unos supuestos específicos las posibilidades de tratamiento, por lo que la interpretación que se realice debe ser restrictiva» (p.9). En lo referente a la calificación de la condición de víctima de violencia de género, la AEPD concluyó que «si bien no estamos ante categorías especiales de datos previstas en el art. 9 RGPD, no puede obviarse que son datos sensibles que requieren la mayor protección, de acuerdo con la eficacia y alcance de un derecho fundamental en relación con la especial consideración que el legislador y, en su caso, los poderes públicos, otorgan al colectivo de víctimas de violencia de genero a través de los distintos cuerpos jurídicos y resoluciones» (p.29).

[214] Conforme al art. 16 (2) TFUE, «El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos».

[215] Amedeo, A. «The Twin Doctrines of Primacy and Pre-Emption», en Schütze, R. y Tridimas, T. *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I,* Oxford Academic, 2018.

Así las cosas, los señalados pronunciamientos de la AEPD son una materialización de que la actual categorización de datos sensibles es inadecuada para el propósito previsto de evitar efectos adversos o discriminatorios, llevando a situaciones en las que las autoridades de protección de datos se aparten de la norma produciendo una grave inseguridad jurídica para los responsables de tratamiento. No se discute que ciertos datos personales como la identidad de género puedan producir efectos discriminatorios. Lo que se discute es si necesitamos una reformulación del sistema actual de datos sensibles.

Volviendo a aquellos datos personales que están claramente excluidos de la lista, debemos señalar la edad. Si bien algunas autoridades nacionales de protección de datos propusieron al GT29 la inclusión de la edad como una categoría sensible bajo una aproximación por riesgo, la misma finalmente se excluyó de la lista[216]. Aunque el tratamiento de datos sobre la edad no siempre conlleva efectos adversos, ya que puede utilizarse positivamente para personalizar anuncios sobre productos que interesen o beneficien al destinatario, también puede ser usado con fines perjudiciales. La cuestión, de nuevo, radica en qué uso se da a dichos datos. Por ejemplo, la edad puede ser un factor para excluir a ciertos destinatarios de anuncios de empleo en diversas plataformas o para explotar una posible menor comprensión tecnológica a través de ciertas condiciones[217].

Otro caso importante de dato personal excluido de la lista es la geolocalización. En Estados Unidos hay diversas normas estatales de privacidad que reconocen la geolocalización como «información personal sensible», sometiendo su tratamiento a normas más estrictas, pero el RGPD no le aplica ningún régimen especial[218]. Si bien las principales preocupaciones respecto a la geolocalización se sitúan en el riesgo de vigilancia masiva por parte de los gobiernos, en el entorno de las prácticas comerciales también puede aparejar efectos adversos[219]. Algunos datos de geolocalización pueden ser *proxies* de datos sensibles, como es el caso de la visita a una clínica abortiva y los datos relacionados con la salud[220]. Otros *proxies* revelan datos que no constituyen información sensible, pero pueden llevar a discriminaciones publicita-

---

[216] Article 29 Data Protection Working Party, «Advice paper on special categories…», *op. cit.*

[217] Rodríguez Escanciano, S. y Gómez García, F. X. «La edad como factor de vulnerabilidad social: algunos factores merecedores de preocupación», *Derecho de las relaciones laborales*, 5, 2018, págs. 505-524.

[218] Entre las normas que reconocen la geolocalización como información personal sensible encontramos la sección § 1798.140(o)(1)(G) de la Ley de Privacidad del Consumidor de California (*California Consumer Privacy Act of 2018*, *«CCPA»);* y la sección §1-(38) de la Ley de Privacidad de Connecticut (*Connecticut Data Privacy Act of 2023, «CTDPA»).*

[219] Solove, D. J. «Data is what data does…», *op. cit.*

[220] Romeo Casabona, C. M. «Datos relativos a la salud…», *op. cit.*

rias. Así, el historial de visitas a determinados restaurantes o a tiendas de lujo puede revelar una mayor capacidad económica, la cual puede determinar precios personalizados más altos[221].

Lo mismo puede suceder en el caso de servicios de transporte como Uber, un señalado ejemplo de modelo de negocio que ha aumentado sus beneficios gracias a las discriminaciones de precios *online*[222]. Algunos estudios sugieren que la discriminación de precios en Uber puede tener resultados finales que mejoren el bienestar general del consumidor al aumentar las opciones de viaje[223]. Otros estudios ponen en entredicho esta perspectiva, argumentando que en ocasiones la discriminación de precios estigmatiza y perjudica a algunos sectores sociales. Un estudio español mostró que las compañías Uber, Cabify y Bolt tienden a fijar precios más altos en barrios con rentas inferiores, al tener menos demanda[224]. Otros estudios revelan que Uber tiende a elevar los precios a aquellos usuarios con baja batería en el móvil, práctica que podría ser discutible éticamente pero no se basa en el tratamiento de datos sensibles[225].

La discriminación de precios nos lleva a destacar otros datos que entrañan graves riesgos de discriminación o efectos económicos adversos: los datos reveladores de la situación financiera. En un estudio llevado a cabo en 2008 en Reino Unido, la mayoría de los encuestados puntuó a los mismos como la categoría más sensible de datos[226]. Pese a las evidentes preocupaciones sociales y los efectos perjudiciales que muchos de sus usos entrañan, no llegaron a incluirse como datos sensibles en el RGPD.

En el ámbito de los anuncios personalizados sobre contratos de préstamo, incluso si una entidad puede explicar qué datos y variables (registros bancarios, ingresos, código postal…) se han utilizado para segmentar a ciertos individuos o personalizar las condiciones anunciadas para cada uno, la decisión se basa en inferencias extraídas

---

[221] Gumbus, A. y Grodzinsky, F. «Era of Big Data: Danger of Discrimination», *SIGCAS Computers & Society,* vol. 45, núm. 3, 2016, pp.118-125; y Pastrana Espárraga, M. «Los precios personalizados como práctica anticompetitiva de discriminación mediante el uso de algoritmos», en Paniagua Zurera, M. (dir.), *El sistema jurídico ante la digitalización: estudios de derecho privado*, 2021, pp. 361-378.

[222] Sherman, L., «Uber's New Math: Increase Prices And Squeeze Driver Pay», *Forbes*, 2023.

[223] Una de las discriminaciones de precios más utilizadas por Uber se da en casos en los que el usuario solicita transporte desde un aeropuerto al hotel. Cuando el hotel es de un precio más elevado, el algoritmo de Uber aplica precios mayores al viajante. *Vid.* Chang, Y., Winston, C. y Yan, J. «Does Uber Benefit Travelers by Price Discrimination?», *The Journal of Law and Economics,* 2018.

[224] Observatorio de Trabajo, Algoritmo y Sociedad, «Adversarial Audit of ride-hailing platforms. Algorithmic compliance with competition, labor and consumer law in Spanish State».

[225] The Brussels Time, «Uber fares allegedly linked to phone battery levels», 2024.

[226] Mccullagh, K. «Data Sensitivity…», *op. cit.*

de estas fuentes. Una inferencia habitual puede ser el grado de fiabilidad del prestatario objetivo. Como señalan ciertos autores, nos encontramos ante una suposición o predicción sobre el comportamiento futuro que no puede ser verificada o refutada en el momento de la toma de decisiones o de la segmentación[227]. Si la selección de los destinatarios se basa en datos no sensibles que meramente sugieran la situación económica actual o futura del individuo, no nos encontraríamos ante un tratamiento de datos sensibles, por mucho que dichos datos puedan dar lugar a efectos adversos, excluyendo a determinados destinatarios de préstamos esenciales para el acceso a una vivienda.

En el ámbito de los anuncios sobre contratos de trabajo también podemos encontrar numerosos ejemplos de efectos adversos para el sujeto de datos. El sistema de IA utilizado por el medio publicitario (como una red social) puede elaborar perfiles con base a datos como la nacionalidad, la geolocalización o el código postal que resulten en la exclusión automática de determinados destinatarios. Bajo la prohibición del art. 26 (3) de la DSA, si los perfiles se basan en datos que no son categorizados como sensibles bajo la lista del RGPD, los mismos podrían utilizarse para presentar publicidad en las plataformas en línea.

Otro ejemplo conflictivo sería el tratamiento de datos que revelen emociones de los individuos. En multiplicidad de ocasiones, la publicidad personalizada se basa en datos comportamentales como el tono de la voz o la frecuencia de los clics, pero los mismos no siempre son datos sensibles biométricos, ya que el uso de ciertos sistemas de reconocimiento de emociones en tiempo real permite evadir la identificación única del individuo, requisito imprescindible para que se aplique la calificación de dato biométrico en el sentido del RGPD[228]. Algunos autores ya venían advirtiendo del peligro de explotar las emociones de los usuarios mediante IA con fines publicitarios[229]. Estos riesgos se han intentado paliar hasta cierta medida a través de la regulación de los sistemas de IA prohibidos y de alto riesgo en la AIA, si bien este Reglamento presenta el mismo vicio: una excesiva dependencia sobre el concepto de datos sensibles biométricos establecido por el RGPD[230].

Todos los ejemplos anteriormente expuestos evidencian cómo el actual sistema de categorización de datos personales entre sensibles y no sensibles es incapaz de hacer frente al propósito original de la regulación especial de los datos sensibles: evitar efectos adversos en los sujetos de datos. Esta incapacidad se traduce en una necesidad de reformular dicho sistema, prestando una mayor atención al uso y no a la recolección o monetización de los datos, actividades que no tienen

---

[227] Solove, D. J. «Data is what data does…», *op. cit.*

[228] Kindt, E. J. «Having yes, using no?…», *op. cit.*

[229] Valcke, P., Clifford, D. y Dessers, V., «Constitutional Challenges in…», *op. cit.*

[230] Czarnocki, J. «Will new definitions…», *op. cit.*

por qué entrañar efectos adversos *per se*. Bajo el principio de libertad de empresa, una prohibición absoluta sobre el tratamiento de dichos datos con fines comerciales o sobre su monetización no resultaría proporcional ni justificada.

Finalizando, podemos concluir dos posibles soluciones. La solución *de lege ferenda* pasaría por una reformulación del sistema actual de datos sensibles, cuyas lagunas regulatorias se han trasladado a la normativa reciente, como la prohibición de la DSA. La solución *de lege lata* sería atender a otros conceptos jurídicos ya existentes que puedan servir para hacer frente a efectos adversos en la publicidad basada en perfiles, como es el concepto de vulnerabilidad.

CAPÍTULO III

ÁMBITO SUBJETIVO DE LA PROHIBICIÓN: LOS PRESTADORES DE PLATAFORMAS EN LÍNEA

I. ACLARACIONES TERMINOLÓGICAS PREVIAS EN TORNO AL CONCEPTO DE PLATAFORMA. DIFERENCIAS RELEVANTES ENTRE LA NOCIÓN DE PLATAFORMAS EN LÍNEA DE LA DSA Y LA DE SERVICIOS BÁSICOS DE PLATAFORMA DE LA DMA

Como adelantábamos en apartados anteriores, el ámbito personal de la prohibición de presentar publicidad basada en perfiles utilizando datos sensibles se circunscribe exclusivamente a los prestadores de plataformas en línea, *entendidas en el sentido de la DSA*. Hacemos particular énfasis en esta última parte, ya que en la práctica frecuentemente se confunden los términos «plataforma en línea» (en torno al cual gira el régimen de la DSA) y «servicio básico de plataforma» (base de la DMA). Antes de analizar el ámbito personal de la prohibición, es preciso aclarar que ambos términos no deben utilizarse como sinónimos puesto que, pese a que ambos sean el objeto central de regulación del Paquete de Servicios Digitales y sus contornos puedan solaparse en determinados aspectos, presentan acusadas divergencias.

1. Diferente ámbito material de ambas categorías: servicios intermediarios (DSA) y servicios de intermediación (DMA)

La primera diferencia entre los conceptos de plataformas en línea y servicios básicos de plataforma radica en su clasificación. La DSA considera a las plataformas en línea como una subcategoría de servicios intermediarios. En cambio, según la DMA, los servicios básicos de plataforma son una categoría general dentro de la cual se incluyen como tipo específico los servicios de intermediación en línea. Esto nos lleva a puntualizar, primeramente, que los conceptos servicios intermediarios (DSA) y servicios de intermediación en línea (DMA) tampoco son sinónimos.

Conforme al art. 3.*g)* de la DSA, un servicio intermediario es uno de los siguientes servicios de la sociedad de la información:

1) Un servicio de *mera transmisión*, consistente en transmitir, en una red de comunicaciones, información facilitada por el destinatario del servicio o en facilitar acceso a una red de comunicaciones. Ejemplos de servicios de mera transmisión son los servicios proveedores de acceso a Internet, los servicios de WiFi, las apps de mensajería instantánea y las autoridades de DNS (*Domain Name System*)[1].

2) Un servicio de *memoria caché*, consistente en transmitir por una red de comunicaciones información facilitada por el destinatario del servicio, que conlleve el almacenamiento automático, provisional y temporal de esta información, prestado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de estos. En otras palabras, los servicios de memoria caché son servicios que almacenan contenido de forma temporal, como es el caso de los proveedores de CDN (*content delivery networks*)[2].

3) Un servicio de *alojamiento de datos*, cuya función es la de almacenar los datos facilitados por el destinatario del servicio y a petición de este. Ejemplos conocidos son las redes sociales, los servicios de intercambio de contenidos, las plataformas de negociación, los foros de discusión, algunos servicios de economía colaborativa, los servicios en la nube, los servicios de alojamiento web y las tiendas de aplicaciones[3].

Cualquiera de los servicios anteriores debe cumplir, a su vez, los requisitos exigidos para ser un servicio de la sociedad de la información, a saber, ser prestado normalmente a cambio de una remuneración,

---

[1] Husovec, M. y Roche Laguna, I., «Digital Services Act…, *op. cit.,* p.4.
[2] *Ibid.*, p.6.
[3] *Ibid.*, p.7.

a distancia, por vía electrónica y a petición individual de un destinatario del servicio[4].

Los servicios de intermediación en línea, en cambio, conforman una subcategoría de servicios básicos de plataforma de la DMA. Para conceptuarlos, la DMA se remite a la definición del art. 2 (2) del Reglamento sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (en adelante, Reglamento P2B)[5], que requiere el cumplimiento cumulativo de los siguientes rasgos:

1) Constituir un servicio de la sociedad de la información, en el sentido de la Directiva sobre comercio electrónico (en adelante DSSICE)[6].

2) Permitir a los usuarios profesionales ofrecer bienes o servicios a los consumidores, con el objetivo de facilitar el inicio de transacciones directas entre dichos usuarios profesionales y consumidores, con independencia de dónde aquellas concluyan en última instancia.

3) Ser prestado a los usuarios profesionales sobre la base de relaciones contractuales entre el proveedor de los servicios y los usuarios profesionales que ofrecen los bienes o servicios a los consumidores.

Confrontando la noción de servicios intermediarios utilizada por la DSA y la de servicios de intermediación empleada por la DMA, podemos evidenciar dos diferencias principales. La primera radica en los usuarios. Mientras que los servicios intermediarios pueden prestarse tanto a usuarios profesionales como a consumidores y usuarios (esto es, desarrollarse B2C o B2B), los servicios de intermediación contemplados por la DMA solo se prestan a usuarios profesionales (P2B).

La segunda diferencia se refiere a lo que podríamos denominar el servicio principal o el servicio caracterizador del concepto. Los servicios intermediarios de la DSA sirven esencialmente como catalizadores de información, pudiendo estar relacionados con la oferta de bienes o servicios —como es el caso de los *marketplace*s y las tiendas de aplicaciones— o no, y calificarse, aun así, como servicios intermediarios —sería el caso, por ejemplo, de los foros de debate—. En cambio, los servicios de intermediación de la DMA deben, en todo

---

[4] Art. 1.1*b)* DSSICE. Márquez Lobillo, P. «El contrato de intermediación electrónica tras los reglamentos europeos sobre transparencia y equidad (p2b), servicios y mercados digitales», en *Revista de derecho mercantil*, núm. 334, 2024.

[5] Reglamento (UE) 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.

[6] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

caso, permitir la oferta de bienes y servicios a consumidores con el objetivo de facilitar transacciones directas[7].

Siguiendo la anterior lógica, es posible que encontremos servicios que reúnan los criterios para encajar en ambas calificaciones —es el caso de *marketplaces* como Booking—, pero también habrá casos en los que el servicio merezca la consideración de servicio intermediario pero no la de servicio de intermediación, al no tener como objetivo facilitar transacciones directas. Un ejemplo sería Wikipedia, reconocida como plataforma en línea de gran tamaño[8]. La falta de ánimo de lucro resulta indiferente para otorgar la calificación de servicio intermediario conforme a la DSA si bien, lógicamente, no se le aplicarán las normas específicas aplicables a las plataformas en línea que permitan la contratación de productos y servicios con consumidores[9].

Concluyendo, podemos subrayar dos notas principales. La primera radica en las divergencias en torno a la categorización. Las plataformas en línea comprenden una subcategoría de servicios intermediarios dentro del ámbito de la DSA, debiendo ser calificadas previa y cumulativamente como: *a)* servicio de la sociedad de la información; *b)* servicio intermediario; y *c)* servicio de alojamiento de datos. Los servicios básicos de plataforma de la DMA, por el contrario, no son una subcategoría, sino que constituyen una categoría general (primer nivel) dentro de la cual se engloban subcategorías tales como los servicios de intermediación y los servicios de publicidad.

La segunda nota principal es que si bien los conceptos de servicio intermediario (DSA) y servicio de intermediación (DMA) no constituyen sinónimos, habrá ocasiones en las que un mismo servicio pueda recaer bajo ambos conceptos, si bien ambos presentan acusadas diferencias en torno a sus destinatarios y el servicio esencial prestado.

2. La designación del prestador del servicio de plataforma

Salvo una excepción (las VLOP), las obligaciones sobre plataformas de la DSA se aplican a todo servicio de plataforma en línea, independientemente de su prestador y sin necesidad de que sea designado como tal. En cambio, las obligaciones sobre plataformas de la DMA solo se aplican a aquellos servicios de plataforma ofrecidos

---

[7] Podszun, R. *Digital Markets Act: Article-by-Article Commentary*, Bloomsbury Publishing 2024, pp. 3-14.

[8] Commission Decision of 25/4/2023 designating Wikipedia as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[9] Husovec, M. «The DSA's Scope Briefly Explained», *SSRN Electronic Journal*, 2023, versión electrónica.

por prestadores que hayan sido designados como guardianes de acceso, siguiendo el procedimiento establecido en el propio Reglamento. Ello resulta, como veremos más adelante, en un ámbito de aplicación mucho más reducido en el caso de la DMA.

En cuanto a su ámbito de aplicación, la DSA se aplica a los servicios intermediarios ofrecidos a destinatarios del servicio que tengan su lugar de establecimiento o estén situados en la Unión, con independencia del establecimiento de los prestadores[10]. Como veíamos anteriormente, dentro de los servicios intermediarios distinguimos la categoría específica de las plataformas *online*, a las cuales se les aplican una serie de obligaciones especiales. En caso de ser designadas como «plataformas de gran tamaño» (en adelante, por sus siglas en inglés, VLOPs) se someterán cumulativamente a una serie de obligaciones adicionales. Con carácter general, si el servicio cumple con los requisitos para ser considerado un servicio de plataforma en línea, el prestador deberá cumplir con:

1) Las disposiciones aplicables a todos los prestadores de servicios intermediarios[11]. Entre ellas, la designación de puntos de contacto con las autoridades de los Estados miembros, con la Comisión y con la Junta, y ciertas obligaciones de transparencia informativa.
2) Las disposiciones adicionales aplicables a los prestadores de servicios de alojamiento de datos, incluidas las plataformas en línea[12]. Por ejemplo, los mecanismos de notificación y acción.
3) Las disposiciones adicionales aplicables a los prestadores de plataformas en línea[13], como aquellas relativas a la transparencia en la publicidad.
4) En su caso, las disposiciones aplicables a los prestadores de plataforma que permitan a los consumidores celebrar contratos a distancia con comerciantes[14], como ciertas obligaciones relativas al cumplimiento desde el diseño (*compliance by design*).
5) En su caso, las obligaciones adicionales de gestión de riesgos sistémicos para prestadores de VLOPs[15], las cuales incluyen obligaciones de auditorías independientes.

Dentro del ámbito personal de la tercera categoría, es decir, las disposiciones adicionales aplicables a los prestadores de plataformas en línea, solo encontramos una excepción: las microempresas y las pequeñas empresas. Conforme al art. 19, las disposiciones aplicables a las plataformas no se aplicarán a los prestadores de plataformas en línea

[10] Art. 2 (1) DSA.
[11] Aquellas contenidas en el capítulo III, sección 1 (arts. 11-15) DSA.
[12] Aquellas contenidas en el capítulo III, sección 2 (arts. 16-18) DSA.
[13] Aquellas contenidas en el capítulo III, sección 3 (arts. 19-28) DSA.
[14] Aquellas contenidas en el capítulo III, sección 4 (arts. 29-32) DSA.
[15] Aquellas contenidas en el capítulo III, sección 4 (arts. 33-43) DSA.

que sean microempresas o pequeñas empresas tal como se definen en la Recomendación 2003/361/CE[16][17]. La excepción a la excepción sería que la pequeña empresa o la microempresa sea designada como una VLOP. Dicha casuística parece bastante improbable en la práctica, ya que tendríamos que encontrarnos ante una plataforma que supere o iguale un promedio mensual de destinatarios del servicio activos en la Unión de 45 millones y, al mismo tiempo, que su volumen de negocios o balance general anual sea inferior a 10 millones de euros (en caso de ser empresa pequeña) o a 2 millones (en caso de ser microempresa)[18].

Salvo que opere la excepción anterior, las obligaciones relativas a las plataformas en línea se aplican a todos los prestadores de servicios de plataforma ofrecidos a destinatarios del servicio que tengan su lugar de establecimiento o estén situados en la UE, independientemente del lugar de establecimiento del prestador[19]. A diferencia del régimen de la DMA, los prestadores de servicios de plataforma se someten a las obligaciones de la DSA automáticamente, sin que sea precisa su designación por la Comisión. En particular, la prohibición de presentar publicidad basada en perfiles utilizando datos sensibles —eje de este trabajo— se aplica directamente a todos los prestadores de plataformas en línea ofrecidos a destinatarios establecidos o situados en la UE, sin necesidad de ningún acto previo de la Comisión. Sólo escapan del ámbito subjetivo de la norma las pequeñas empresas y las microempresas.

La aplicación de las normas de la DMA sigue un procedimiento de aplicación diferente. En este caso, el servicio en cuestión no solo deberá ser uno de los servicios básicos de plataforma indicados por el art. 2 (2) DMA, sino que además deberá ser ofrecido por una empresa a la que se designe como guardián de acceso. Así lo exige la DMA al indicar en su art. 1.2 que el Reglamento «se aplicará a los servicios básicos de plataforma prestados u ofrecidos por guardianes de acceso a usuarios profesionales establecidos en la Unión o a usuarios finales establecidos o situados en la Unión, independientemente del lugar de establecimiento o residencia de los guardianes de acceso y del derecho que, por lo demás, sea aplicable a la prestación del servicio».

---

[16] Conforme al art. 2 (2) de la Recomendación, una pequeña empresa es aquella que ocupa a menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 10 millones de euros. Una microempresa, conforme al art. 2 (3), es aquella que ocupa a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 2 millones de euros.

[17] Con excepción del art. 24 (3), relativo a ciertas obligaciones de transparencia informativa a requerimiento del coordinador de servicios digitales de establecimiento y de la Comisión.

[18] Art 33 (1) DSA.

[19] Art 2 (1) DMA. Benavides Velasco, P. «The position of the Court of Justice of the European Union on services provided by digital platforms in the tourism sector», en *Journal of Tourism and Heritage Research: JTHR*, vol. 4, núm. 2, 2021 (Ejemplar dedicado a: Journal of Tourism and Heritage Research), p. 189.

En otras palabras, a diferencia de la DSA, para que las obligaciones de plataforma de la DMA resulten aplicables, el servicio debe cumplir un doble requisito: *a)* constituir una de las categorías de servicio básico de plataforma del art. 2 (2) DMA y *b)* ser prestado u ofrecido por un guardián de acceso. El guardián de acceso es definido, a su vez, como «una empresa prestadora de servicios básicos de plataforma, designada de conformidad con el artículo 3»[20].

Si bien no es objeto del presente trabajo profundizar en el procedimiento para designar a un guardián de acceso, es reseñable que nos encontramos ante un proceso complejo instruido por la Comisión Europea[21]. Según el art. 3.1 DMA para considerar la designación de una plataforma como guardián de acceso se deberán cumplir tres requisitos:

a) que tenga una gran influencia en el mercado interior;

b) que preste un servicio básico de plataforma que es una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales, y

c) que tenga una posición afianzada y duradera, por lo que respecta a sus operaciones, o es previsible que alcance dicha posición en un futuro próximo.

Para aportar seguridad jurídica y facilitar su aplicación, el art. 3.2, establece la presunción de que dichos requisitos se cumplen cuando:

a) en relación con el apartado 1, letra *a)*, cuando la empresa consiga un volumen de negocios anual en la Unión igual o superior a 7 500 000 000 euros 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 euros en el último ejercicio, y preste el mismo servicio básico de plataforma en al menos tres Estados miembros;

b) en relación con el apartado 1, letra *b)*, cuando proporcione un servicio básico de plataforma que, en el último ejercicio, haya tenido al menos 45 000 000 mensuales de usuarios finales activos establecidos o situados en la Unión y al menos 10 000 usuarios profesionales activos anuales establecidos en la Unión, identificados y calculados de conformidad con la metodología y los indicadores establecidos en el anexo;

c) en relación con el apartado 1, letra *c)*, cuando se hayan alcanzado los umbrales establecidos en la letra *b)* del presente apartado en cada uno de los últimos tres ejercicios.

---

[20] Art. 2 (1) DMA.

[21] Olmedo Peralta, E. «Redefiniendo el ámbito de aplicación de la Ley de Mercados Digitales: ¿a quién?, ¿cómo? y ¿para qué?», en Tato Plaza, A. *et al.* (dirs), *Nuevas tendencias en el derecho de la competencia y de la propiedad industrial III,* 2022, Comares, pp. 87-116.

Como señalan algunos autores, el poder de la Comisión para que operen o no las obligaciones de la DMA es apreciable en un gran número de disposiciones del articulado[22]. Entre ellas, destaca la posibilidad de que se designe como gatekeeper a una plataforma, aunque no se cumplan las presunciones del apartado segundo, si la Comisión concluye que se cumplen todos los requisitos generales del apartado primero[23][24]. En sentido contrario, también es posible que se cumplan todas las presunciones, pero la Comisión decida no designar a la empresa como guardián de acceso si, en vista de los argumentos presentados por el prestador, concluye que no concurren los requisitos generales del apartado primero[25][26].

Retornando al concepto de plataforma, destaca no solo que el servicio básico de plataforma deba ser prestado por un guardián de acceso designado como tal, sino que además el servicio de plataforma en cuestión debe ser designado por la Comisión como «una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales», en la misma decisión en la que designa a la empresa como guardián de acceso[27][28]. Un ejemplo sería el de *TikTok Ads*. Si bien la empresa *ByteDance* fue designada por la Comisión como guardián de acceso, designando a la red social *TikTok* como servicio básico de plataforma, la Comisión decidió no designar como plataforma a otro de sus servicios, *Tik Tok Ads*[29]. La razón alegada por la Comisión fue precisamente que el servicio no constituía una puerta de acceso importante pese a que la empresa cumpliese los requisitos cuantitativos, a diferencia del caso de *Google Ads*.

---

[22] Por todos, *vid.* Olmedo Peralta, E. «La construcción de un régimen jurídico para el sector digital más allá del reglamento de mercados digitales», en Rodilla Martí, C. y Ruiz Peris, J. I. (coord.), *Mercados digitales y competencia*, Tirant lo Blanch, 2022, pp. 153-208, y Cennamo, C. *et al.,* «Digital Platforms Regulation: An Innovation Centric View of the EU's Digital Markets Act», *Journal of European Competition Law & Practice*, 2023.

[23] Arts. 3 (8) y 17 DMA.

[24] Olmedo Peralta, E. «Las plataformas de economía colaborativa ante la propuesta de ley de mercados digitales: ¿Son suficientemente disputables los mercados colaborativos?», en Miranda Serrano, L. M. y Pagador López, J. (dirs.), *Desafíos del regulador mercantil en materia de contratación y competencia empresaria*l, Marcial Pons, 2021, pp. 359-380.

[25] Art. 3(5) DMA.

[26] Olmedo Peralta, E. «How does Android protects its dominance in the mobile ecosystem, and why might the Digital Markets Act not be enough? concerns on alphabet practices on operating system», en Ruiz Peris, J. I. y Estevan de Quesada, C. *New European Competition Trends in Digital Markets*, Atelier, 2024, pp. 209-235.

[27] Art. 3 (9) DMA.

[28] Olmedo Peralta, E. «El reto de adaptar el derecho de la competencia a la lógica de la economía de los datos», en Olmedo Peralta, E. (dir.), *La aplicación del derecho de la competencia en la economía de los datos*, Aranzadi, 2021.

[29] Commission Decision of 25/4/2023 designating TikTok as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

Concluyendo, para considerar que una empresa que opera un servicio básico de plataforma es un gatekeeper se han de reunir unos requisitos elevados: *a)* ser uno de los servicios incluidos en la lista del art. 2(2) DMA; *b)* ser prestado por un guardián de acceso designado como tal y *c)* constituir una puerta de acceso *importante*.

Por ello, naturalmente, las obligaciones impuestas por la DMA a las plataformas se aplicarán de una forma excepcional, frente al régimen generalizado de aplicación de la DSA, dado que los requisitos de calificación como plataforma en línea de la DSA son mucho más laxos.

3. El servicio caracterizador

La tercera diferencia esencial entre los conceptos de plataforma ofrecidos por la DSA y la DMA radica en los servicios que comprende cada concepto. Un servicio de plataforma en línea, en el sentido de la DSA, comprende servicios de intermediación que cumplan con los siguientes requisitos[30]:

1) Ser un servicio de alojamiento de datos, en el sentido del art. 3.*g)* de la DSA, es decir, ser un servicio consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este.

2) Ser prestado a petición de un destinatario del servicio. La concurrencia de este requisito aporta un carácter circular a la definición, puesto que ya es exigido para ser un servicio de la sociedad de la información y, como exponíamos anteriormente, todo servicio de plataforma de la DSA debe ser calificado como un servicio de la sociedad de la información. En sede de la DSA, un destinatario del servicio es definido como toda persona física o jurídica que utilice un servicio intermediario, en particular para buscar información o para hacerla accesible[31]. La DSA opta así por un concepto amplio que englobe todo tipo de operadores: tanto a los usuarios profesionales como a los consumidores y usuarios que hagan uso de la plataforma[32].

3) Que el servicio consista en almacenar y difundir información al público. Como bien señala el considerando 13 de la DSA, para que un servicio de alojamiento de datos sea un servicio de plataforma en línea no debe solo alojar dicha información, sino que debe cumplir un requisito adicional: difundirla al público.

---

[30] Art. 3 (i) DSA.

[31] Art. 3 (b) DSA.

[32] Por ejemplo, en el caso de plataformas de alojamiento tales como Booking o AirBnB se englobarían como destinatarios del servicio: los usuarios profesionales que ofertan alojamiento en la plataforma y los destinatarios finales, independientemente de si estos últimos son calificados como consumidores o como profesionales.

4) Se incluye como excepción que esa actividad —el almacenamiento y difusión de información al público— sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad accesoria 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 de la DSA.

En suma, la DSA no establece una lista taxativa de servicios considerados de plataforma, sino que establece una serie de requisitos para merecer tal consideración. La DMA, por contra, toma una aproximación bastante distinta, ya que establece en su art. 2.2 una lista cerrada de lo que considera *servicios básicos de plataforma* que podrán servir de base para la designación de *gatekeepers* por la Comisión[33]. Dicha lista está constituida por:

1) Los servicios de intermediación en línea, en el sentido del art. 2(2) del Reglamento P2B[34]. Esta categoría engloba una gran variedad de servicios, algunos ejemplos son Google Maps, Google Play y Google Shopping (prestados por el guardián de acceso Alphabet)[35] o AppStore (Apple)[36]. La inclusión de las tiendas de aplicaciones es especialmente relevante, ya que son la puerta de entrada para que los desarrolladores de aplicaciones puedan poner estas a disposición de los usuarios de teléfonos móviles[37].

2) Los motores de búsqueda en línea[38], como Google Search (Alphabet).

---

[33] Art. 3 (9) DMA.

[34] Es decir, aquellos servicios que cumplan los siguientes requisitos: *a)* ser un servicio de la sociedad de la información; *b)* permitir a los usuarios profesionales ofrecer bienes o servicios a los consumidores, con el objetivo de facilitar el inicio de transacciones directas entre dichos usuarios profesionales y consumidores, con independencia de dónde aquellas concluyan en última instancia; y *c)* ser prestados a los usuarios profesionales sobre la base de relaciones contractuales entre el proveedor de los servicios y los usuarios profesionales que ofrecen los bienes o servicios a los consumidores.

[35] Commission Decision of 5/9/2023 designating Alphabet as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

[36] Commission Decision of 5/9/2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

[37] Olmedo Peralta, E. «Entornos Informáticos: Sistemas Operativos, Tiendas de Aplicaciones, Asistentes Virtuales y Aplicaciones», en Montero Pascual, J. J. (coord) *La regulación de los servicios digitales,* Tirant lo Blanch, 2024, pp.349-406.

[38] Definidos por remisión al art. 2 (5) del Reglamento P2B como aquellos servicios digitales que permiten a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web, o de sitios web en un idioma concreto, mediante una consulta sobre un tema cualquiera en forma de palabra clave, consulta oral, frase u otro tipo de entrada, y que en respuesta muestra resultados en cualquier formato en los que puede encontrarse información relacionada con el contenido solicitado.

3) Los servicios de redes sociales en línea, como Facebook e Instagram (Meta) y LinkedIn (Microsoft)[39].

4) Los servicios de plataforma de intercambio de vídeos[40], como YouTube (Alphabet).

5) Los servicios de comunicaciones interpersonales independientes de la numeración[41], también denominados OTT services (*over-the-top services*)[42]. Algunos ejemplos de estos servicios son WhatsApp y Messenger (Meta).

6) Los sistemas operativos[43], como Google Android (Alphabet).

7) Los navegadores web[44], como Chrome (Google) y Safari (Apple).

8) Los asistentes virtuales[45]. Aunque ninguno de estos servicios ha sido designado como un servicio básico de plataforma

---

[39] Los mismos son definidos ampliamente por el art. 2 (7) DMA como aquellas plataformas que permiten que los usuarios finales se conecten y se comuniquen entre sí, compartan contenidos y descubran contenidos y a otros usuarios a través de múltiples dispositivos y, en particular, mediante chats, publicaciones, vídeos y recomendaciones.

Respecto a Meta y Microdoft *vid.* Commission Decision of 5/9/2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

[40] Definidos por remisión al art. 1.(1).*a) bis* de la Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (en adelante, Directiva de Servicios de Comunicación Audiovisual). La misma define estos servicios como aquellos servicios, «tal como lo definen los artículos 56 y 57 del TFUE, cuya finalidad principal propia o de una de sus partes disociables o cuya funcionalidad esencial consiste en ofrecer al público en general programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretener o educar, a través de redes de comunicaciones electrónicas tal como se definen en el art. 2, letra *a)*, de la Directiva 2002/21/CE, y cuya organización determina el prestador de la plataforma de intercambio de vídeos, entre otros medios con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación».

[41] Definidos por remisión al art 2. (7) del Código de las Comunicaciones Electrónicas como aquellos servicios de comunicaciones interpersonales que no conectan a través de recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional, o no permiten la comunicación con un número o números de los planes de numeración nacional o internacional.

[42] De Streel, A. y Hocepied, C. «The Regulation of Electronic Communications Networks and Services» in Garzaniti, L., O'Regan, M., De Streel, A. y Valcke, P. *Electronic Communications, Audiovisual Services and the Internet*, Sweet and Maxwell, 2019, p.25-123.

[43] Definidos por el art. 2 (10) DMA como softwares de sistema que controlan las funciones básicas del hardware o del software y permiten que se ejecuten en ellos aplicaciones informáticas.

[44] Definidos por el art. 2 (11) DMA como aplicaciones informáticas que permiten a los usuarios finales acceder a contenidos web alojados en servidores que están conectados a redes como internet e interactuar con dichos contenidos, incluidos los navegadores web independientes y los navegadores web integrados en software o similares.

[45] Definidos por el art. 2 (12) DMA como aquellos softwares que pueden procesar peticiones, tareas o preguntas, también las formuladas mediante sonidos, imágenes, texto, gestos o movimientos y que, basándose en dichas peticiones, tareas o preguntas, proporcionan acceso

prestado por un guardián de acceso con base en la DMA, un estudio de la Comisión Europea indica que los líderes del sector son Alexa (Amazon), Google Assistant (Google) y Siri (Apple)[46][47].

9) Los servicios de computación en nube[48]. Hasta la fecha ninguno ha sido designado por la Comisión como un servicio básico de plataforma prestado por un guardián de acceso.

10) Los 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 demás servicios básicos de plataforma. En otras palabras, los servicios de publicidad en línea, a efectos de la DMA, solo podrán ser considerados servicios de plataforma si son prestados por una empresa que preste un servicio básico de plataforma distinto al de publicidad. Por ejemplo, Meta (designada como guardián de acceso) presta tanto servicios básicos de plataforma de publicidad (Meta Ads) como servicios de red social (Facebook e Instagram). Al prestar servicios de red social, su servicio de publicidad pudo ser designado como servicio básico de plataforma, si bien otros factores determinantes fueron ser considerado por la Comisión como una puerta de acceso importante y cumplir los requisitos cuantitativos[49].

Haciendo una comparativa entre los servicios de plataforma de la DSA y de la DMA, conviene concluir que, en la práctica, no todos coincidirán. Por un lado, es cierto que algunos servicios quedan amparados por ambas normas, al cumplir con los requisitos para ser considerados plataforma a efectos de la DSA y haber sido designados por la Comisión como servicios básicos de plataforma conforme a la DMA. Este sería el caso de redes sociales como Facebook, Instagram y LinkedIn, o de plataformas de intercambio de vídeos como YouTube, todos ellos designados como servicios básicos de plataforma conforme a la DMA y como VLOP (una subcategoría especial dentro de las plataformas) conforme al procedimiento de la DSA.

---

a otros servicios o controlan dispositivos físicos conectados. La misma definición es acogida, verbatim, por la AIA en su art. 2 (31).

[46] European Commission, *Preliminary Report – Sector Inquiry Into Consumer Internet Of Things,* 2021, p.5.

[47] Ovington, R. / Lewis, D. «Virtual assistants and the DMA», 2022.

[48] Definidos por remisión al art. 4(19) de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Un servicio de computación en nube es definido por la Directiva como «un servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos informáticos que se pueden compartir».

[49] Commission Decision of 5/9/2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

Por otro lado, encontramos otros servicios que han sido designados como servicios básicos de plataforma conforme a la DMA y que, sin embargo, no son una plataforma a efectos de la DSA, por no cumplir el requisito de difundir información al público. Este sería el caso, por ejemplo, de sistemas operativos como Google Android e iOS, o de servicios OTT como WhatsApp y Messenger[50].

Por último, cabe destacar la posibilidad de que ocurra la casuística contraria, es decir, que un servicio sea una plataforma en línea en el sentido de la DSA, pero no sea designado como un servicio básico de plataforma por la Comisión bajo la DMA, ya que los objetivos de ambas normas, si bien complementarios, son totalmente distintos[51]. Esta divergencia puede concurrir, en líneas generales, por una o varias de las siguientes causas: *a)* no ser prestado por un gatekeeper, *b)* no encajar en ninguna de las categorías de servicios de plataforma del art. 2(2) DMA; o *c)* no ser considerado por la Comisión como una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales.

Un ejemplo de la primera causa sería AliExpress. Si bien cumple con los requisitos para ser considerada plataforma a efectos de la DSA (de hecho, fue designada por la Comisión como una VLOP)[52], el prestador principal, Alibaba Group Holding Limited (Grupo Alibaba), no ha sido designado hasta la fecha como guardián de acceso, por lo que el servicio AliExpress no podría quedar sujeto a las obligaciones de la DMA, ya que la empresa prestadora no ha sido designada como guardián de acceso.

Un ejemplo de concurrencia de las dos primeras causas sería Wikipedia. Por un lado, la empresa prestadora, Wikimedia Foundation, Inc., no ha sido designada hasta la fecha como guardián de acceso. Por otro lado, el servicio en cuestión no queda compren-

---

[50] Definidos por remisión al art 2. (7) del Código de las Comunicaciones Electrónicas como aquellos servicios de comunicaciones interpersonales que no conectan a través de recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional, o no permiten la comunicación con un número o números de los planes de numeración nacional o internacional.

[51] En líneas generales, el objetivo de la DMA es garantizar la equidad y la disputabilidad de los mercados en el sector digital donde haya guardianes de acceso, mientras que el propósito principal de la DSA es crear un entorno en línea seguro, predecible y fiable que facilite la innovación y en el que se protejan efectivamente los derechos fundamentales. Para un examen comparativo sobre los propósitos de ambos reglamentos. *vid.* Di Porto, F. *et al.* «I see something you don't see. A computational analysis of the DMA and DSA», *Computational Antitrust Journal*, 2021; y Hobbelen, H. Cunningham, F. y Denihan, C. «The European Commission's Ambitious Regulatory Agenda in the Field of Digital Services and AI: a status update from Brussels on the DSA, DMA and AI Act», *IBA*, 2021.

[52] Commission Decision of 25/4/2023 designating AliExpress as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

dido en ninguna de las categorías de servicio básico de plataforma del art. 2.2 DMA, ni siquiera en el concepto de servicio intermediario, ya que el objetivo de Wikipedia es meramente compartir información, no facilitar el inicio de transacciones directas entre dichos usuarios profesionales y consumidores[53]. En consecuencia, Wikipedia no estaría sujeta a las obligaciones de la DMA, pero sí quedaría sujeta a las obligaciones de la DSA, al ser una plataforma en línea en el sentido de esta última e incluso haber sido designada como VLOP[54].

Un ejemplo de la tercera causa sería TikTok Ads. Si bien TikTok Ads es prestado por un guardián de acceso (*ByteDance*) y el servicio es un servicio de publicidad, comprendido en la lista del art. 2(2) DMA, este no fue designado como servicio básico de plataforma al concluir la Comisión que no constituía una puerta de acceso importante[55].

En conclusión, si bien habrá ocasiones en las que un servicio sea considerado plataforma a efectos de ambas normas, habrá ocasiones en las que a un mismo servicio solo se le aplique la DMA o solo se le aplique la DSA, ya que las definiciones de plataforma bajo ambas (en coherencia con sus respectivos objetivos) son sensiblemente diferentes.

II. LA REFORMULACIÓN DEL TÉRMINO «DIFUSIÓN AL PÚBLICO», EN LA DSA. ¿EXCLUSIÓN DE CIERTOS SERVICIOS?

En el apartado anterior, apuntábamos brevemente que un servicio de alojamiento de datos solo será considerado una plataforma en línea si, además de alojar datos, los difunde al público. Es necesario que nos detengamos en este requisito, ya que el concepto de *público* puede constituir una de las mayores vías de escape de las obligaciones de la DSA, entre ellas, la prohibición de presentar publicidad basada en perfiles usando datos sensibles.

Previamente a la entrada en vigor de la DSA, tanto la doctrina como la jurisprudencia del TJUE venían entendiendo el concepto de público como un número «indeterminado y considerable» de personas[56]. Si bien

---

[53] Como exige el art. 2 (2) DMA por remisión al art. 2(2) del Reglamento P2B.

[54] Commission Decision of 25/4/2023 designating Wikipedia as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[55] Commission Decision of 25/4/2023 designating TikTok as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[56] Por todos, ver asuntos acumulados CJEU C-682/18 and C-683/18, *YouTube and Cyando*, ECLI:EU:C:2021:503, párrafo 69. En el mismo sentido se pronuncia la doctrina, entre ellos Pila, J. y Torremans, P. L. C. «The law of copyright and related rights» in Pila, J. y Torremans, P. L. C., *European Intellectual Property Law*, Oxford, 2019, pp. 295-300; Peinado Gracia, J. I.

esta consolidada interpretación se había desarrollado en el ámbito de los derechos de autor, no debemos ignorar que uno de los objetivos principales de la DSA es combatir la difusión de contenidos ilícitos en línea, lo que incluye la difusión de contenidos que infrinjan tales derechos[57-58]. Viendo la estrecha relación entre los propósitos de la DSA y la normativa de derechos de autor, hubiera sido coherente que se hubiese optado por una de las siguientes opciones: *a)* que la DSA no contuviese una definición propia del término difusión al público, lo que hubiese dado lugar a la remisión al concepto de *público* del TJUE como concepto autónomo; o *b)* que se integrase *verbatim* la definición del TJUE, opción que no es nada insólita en la normativa de la UE[59].

En contra de la sana coherencia, el legislador decidió incluir en la DSA una definición propia de público, definiéndolo en el art. 3.*k)* como *un número potencialmente ilimitado de terceros*. La diferencia es grave: al aludir a un número potencialmente ilimitado, se ha optado por un concepto mucho menos flexible, ya que excluye a servicios que fijen un número máximo de destinatarios, por elevado que pueda ser ese número.

El considerando 14 de la norma acentúa todavía más esta falta de flexibilidad, al excluir expresamente del concepto de plataforma a: *a)* los grupos de destinatarios que requieran inscripción o admisión, cuando no resulte automática y sea un humano quien decida o escoja a quién se concede acceso; y *b)* los servicios de comunicaciones interpersonales definidos en el Código Europeo de Comunicaciones

---

«La propiedad intelectual: derechos de autor y derechos afines», en Menéndez Menéndez, A. (dir.) y Rojo Fernández Río, A. J. (dir.), *Lecciones de derecho mercantil*, 2024, pp. 239-277; Galacho Abolafio, A. F. «Contenidos digitales y su puesta a disposición a través de Internet a la luz de las últimas sentencias del TJUE: el papel fundamental del concepto de agotamiento del derecho», en Miranda Serrano, L. M. y Pagador López, J. (dirs.), *Contratación mercantil: digitalización y protección del cliente-consumidor*, 2023, pp. 75-92;

[57] El concepto de «público» ha sido interpretado por el Alto Tribunal en el marco del art. 3 (1) de la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.

[58] La DSA no establece concretamente qué es un contenido ilícito, limitándose a señalar en su art. 3 (h) que es «toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el derecho de la Unión o el derecho de cualquier Estado miembro que cumpla el derecho de la Unión, sea cual sea el objeto o carácter concreto de ese derecho». Sin embargo, aporta algunos ejemplos en su considerando (12), como «el uso no autorizado de material protegido por derechos de autor». El legislador no ha sido ajeno a que la mayoría de los contenidos ilícitos en línea son aquellos que infringen derechos de autor, como bien indican informes de transparencia aportados por prestadores como Google. En este sentido, *vid.* Google, «Informe de transparencia. Retirada de contenido por infracciones de derechos de autor», 2024.

[59] Sánchez Frías, A. *Los conceptos autónomos en el derecho de la Unión Europea*, Tirant lo Blanch, 2023, p.27.

Electrónicas[60], como los correos electrónicos o los servicios de mensajería privada. La primera exclusión obedece a que el considerando exige que la información sea fácilmente accesible al público, requisito que se presume incumplido cuando el acceso al grupo no es automático y debe ser aceptado por un humano. La segunda exclusión responde a la definición de público como un *número indeterminado* de destinatarios, ya que los servicios de comunicaciones interpersonales, por definición, quedan circunscritos a un número finito de personas[61].

La exigencia de que la información se difunda a un número potencialmente ilimitado de personas ha suscitado acaloradas críticas de buena parte de la doctrina, más favorable a incorporar el concepto de público que venía defendiendo el TJUE, argumentando que se hubiese evitado excluir canales que implican los mismos riesgos que la DSA pretende paliar[62].

Un claro ejemplo serían los grupos de Telegram, que estarían excluidos del concepto de plataforma al presentar la limitación de 200 000 miembros, así como por ser un servicio de comunicaciones interpersonales. A nuestro entender, es cuestionable por qué un grupo público de Facebook está sometido a las normas de la DSA sobre plataformas en línea, mientras que un grupo de Telegram no, cuando ambos pueden alcanzar a un número considerable de personas, teniendo un impacto potencial importante en la difusión de contenidos ilícitos y otros riesgos que la DSA pretende paliar.

Otro caso problemático sería la creación de servicios por suscripción o inscripción en los que se establezca una limitación técnica de miembros excesivamente alta con el objeto de evitar la aplicabilidad de la norma. Si atendemos a la literalidad de la DSA, aunque el número máximo fuese extremadamente elevado (por ejemplo, 100 millones de miembros), el servicio en cuestión no sería una plataforma en línea y, en consecuencia, no estaría sujeto a las normas aplicables a estas. En esta línea, el considerando 44 parece tendente a excluir todo servicio limitado a un número finito de personas. Algunos ejemplos serían

---

[60] Art. 2 (5) de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (*DO* L 321 de 17/12/2018, p. 36); (en adelante, Código Europeo de las Comunicaciones Electrónicas). Conforme al art. 2 (5) del Código Europeo de Comunicaciones Electrónicas, un servicio de comunicaciones interpersonales es «el prestado por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio».

[61] Art. 2 (5) del Código Europeo de las Comunicaciones Electrónicas.

[62] Para una crítica más detallada al concepto de «público» de la DSA desde la perspectiva de los derechos de autor, *vid.* Peukert, A. *et al.*, «Comment on Copyright and the Digital…», *op. cit.,* p. 358-376.

los servicios de correo electrónico (Outlook y Gmail tienen un límite de 500 destinatarios por mensaje)[63], o los servicios de mensajería (WhatsApp permite grupos de hasta 1024 miembros)[64]. Desde una política legislativa de aproximación por riesgo, podría parecer justificado que la norma no regule casos en los que el número de destinatarios máximo sea un número moderado, como ocurre con Outlook, Gmail o WhatsApp.

Sin embargo, cabe plantearse si esta interpretación debe aplicarse tanto a servicios con límites modestos como a servicios con límites más elevados. Sería argumentable que el establecimiento de un límite extremadamente alto o incluso irrealizable puede ser un simple medio para evadir la aplicabilidad de la norma y cometer un fraude de ley. Esta cuestión, a nuestro entender, podría dar lugar a posibles cuestiones prejudiciales ante el TJUE, planteando si el requerimiento de público ilimitado previsto por la DSA ampara o no límites excesivamente altos que vayan en contra de su espíritu.

Algo más claro sería el caso de emplear a humanos en el proceso de inscripción para admitir a todo aquel que desee acceder, sin prever motivos de rechazo, con el mero objeto de aplicar una de las exclusiones del considerando 14[65]. Se trataría de un supuesto más evidente de fraude de ley, ya que el objetivo de la norma, al definir el concepto de difusión al público, es abarcar información fácilmente accesible, condición que se daría si la aceptación no está sujeta a requisitos reales. Hablaríamos entonces de casos donde la intervención humana es irrelevante y equiparable al uso de medios automáticos, al emplearse con el simple propósito de evitar las obligaciones que resultarían aplicables. En otras palabras, como parece que el protagonismo se sitúa en que el acceso a la información sea fácil y automático, este requisito se cumpliría aun si el único papel de la intervención humana fuera evitar la aplicabilidad de la norma.

Salvando este último caso, cabe concluir que la reformulación del concepto de difusión al público bajo la DSA puede resultar pro-

---

[63] Soporte técnico de Microsoft, «Límites de envío en Outlook.com», disponible en *https://support.microsoft.com/es-es/office/l%C3%ADmites-de-env%C3%ADo-en-outlook-com-279ee200-594c-40f0-9ec8-bb6af7735c2e*; y Servicio Support de Google, «Límites para enviar y recibir correos electrónicos», disponible en *https://support.google.com/mail/answer/22839?hl=es-419#zippy=%2Calcanzaste-el-l%C3%ADmite-de-env%C3%ADos-de-correo-electr%C3%B3nico.*

[64] WhatsApp Help Center, «Cómo crear un grupo e invitar a participantes», disponible en *https://faq.whatsapp.com/3242937609289432/?locale=es_LA&cms_platform=android.*

[65] Conforme al tenor del considerando (14) DSA «cuando el acceso a la información requiera la inscripción o la admisión en un grupo de destinatarios del servicio, solo debe considerarse que dicha información ha sido difundida al público cuando los destinatarios del servicio que deseen acceder a la información se inscriban o sean admitidos automáticamente sin que un ser humano decida o escoja a quién se concede el acceso».

blemática. Aquellos servicios intermediarios que alojen y difundan información quedan excluidos de las obligaciones aplicables a las plataformas en línea si dicha actividad se realiza a un número técnicamente limitado de personas, por elevado que sea dicho número, salvo posibles pronunciamientos del TJUE en lo que respecta al alcance de la noción de difusión al público.

III. LA DELIMITACIÓN DE LOS SERVICIOS INTEGRADOS BAJO LA PERSPECTIVA DE LA DSA

1. Perspectivas unitarias. Tendencias a considerar el servicio de publicidad y el servicio principal como un servicio «indisoluble»

En los últimos años, el modelo económico de muchos servicios *online* ha sufrido un viraje hacia un nuevo modelo, denominado *advertising-based-business-model*, o modelo de negocio basado en la publicidad. Aunque siempre ha sido común que muchos servicios *offline* (como los periódicos físicos o la televisión) basen una gran parte de sus ingresos en la publicidad, con la aparición de Internet este modelo ha evolucionado, ya que la publicidad ha pasado de ser un mero complemento económico para el prestador del servicio a constituir la fuente principal o incluso exclusiva de sus ingresos[66]. La posibilidad de aumentar la eficacia de la publicidad a través del uso de datos personales con fines de personalización ha causado, igualmente, que muchos prestadores moneticen los datos personales de sus usuarios. Así, un gran número de estudios de mercado señala que no resulta en absoluto comparable el mercado de la publicidad digital con otras formas de publicidad, debido a que no existe una relación de sustituibilidad entre ambos y al nivel de personalización al que puede llegar la primera[67]. En consecuencia, nos encontraríamos ante dos mercados diferenciados[68].

Las fuentes de datos personales y no personales que alimentan la publicidad digital pueden ser muy variadas, abarcando desde ser-

---

[66] Olmedo Peralta, E. «Condiciones para la concesión de licencias sobre el sistema operativo móvil android: Tying, self-preferencing y acuerdos de reparto de ingresos por publicidad (revenue sharing agreements)», *Actas de derecho industrial y derecho de autor*, tomo 44, 2024, pp. 275-299.

[67] CMA, *Online platforms and digital advertising*, *op. cit.*

[68] Comisión Europea, «Comunicación de la Comisión relativa a la definición de mercado de referencia a efectos de la normativa de la Unión en materia de competencia», *DOUE* núm. 1645, 2024, pp. 1-35. Para un análisis de la comunicación, *vid.* Aido Vázquez, A. M. «La delimitación de los mercados digitales: una aproximación a la nueva comunicación de la Comisión Europea», en Tato Plaza, A.; Costas Comesaña, J.; Fernández Carballo-Calero, P.; Louredo Casado, S.; Torres Pérez, F. J. (coords.), *Nuevas tendencias en el Derecho de la Competencia y de la Propiedad Industrial e Intelectual IV*, 2024, pp. 27-66.

vicios que no son de plataforma en línea (como servicios de nube, mensajería digital o *apps* de bancos) hasta servicios de plataforma de gran tamaño, como Facebook, Instagram o Google. Si bien la fuente puede ser variada, el mercado de la publicidad digital se encuentra muy concentrado, ocupando Meta y Alphabet posiciones de dominio muy robustas[69].

Aunque el mayor nivel de ingresos de estos guardianes de acceso se base en la publicidad digital y la monetización de los datos de sus usuarios, no debemos pasar por alto que la exposición a la publicidad digital pasa inevitablemente por el acceso previo o simultáneo a otros servicios prestados por el mismo proveedor. Estas plataformas desarrollan importantes redes de conexión directa entre los servicios digitales que ofrecen, a través de prácticas de *tying* y *bundling*. En muchos casos, se llegan a construir ecosistemas que actúan como jardines vallados (*walled gardens*) produciendo un efecto *lock-in* de sus usuarios[70].

Poniendo un ejemplo, los anuncios mostrados en Facebook solo son accesibles al usuario cuando el mismo inicia sesión en la red social. Lo mismo sucede con Google Search: los resultados calificados como «contenido promocionado» o «anuncio» solo se muestran si el usuario realiza una búsqueda. No es nada comparable, reiteramos, este tipo de publicidad con la publicidad *offline*. Si bien *offline* los destinatarios pueden ser expuestos a publicidad aislada en pósteres, carteles o folletos, la publicidad digital viene siempre aparejada a otro servicio digital. En la diferenciación también impactará —incluso con más fuerza— el hecho de que la publicidad digital casi siempre sea una publicidad customizada o dirigida a cada usuario en particular en función del perfil construido a partir de sus intereses. Nos centraremos más adelante en este aspecto.

Este aparejamiento digital es frecuentemente señalado por los prestadores de servicios de plataforma para sostener la unidad e indivisibilidad de su servicio de publicidad con el servicio principal. Aunque viene de largo, uno de los casos más señalados en los que un guardián de acceso intentó argumentar la indivisibilidad de sus servicios fue el de Meta, con ocasión de una disputa planteada ante el CEPD por infracción del RGPD en lo referente a las bases legales aplicadas para el tratamiento de datos en Instagram con fines de publicidad comportamental[71]. En este caso, Meta había basado el tratamiento en la base legal de necesidad para la ejecución del contrato (art. 6.1.*b)* RGPD).

---

[69] Cabral, L. *et al.*, *The EU Digital Markets Act: A Report from a Panel of Economic Experts*, Publications Office of the European Union, 2021.

[70] Olmedo Peralta, E. «El reto de adaptar el derecho…», *op. cit.*

[71] CEPD Decisión vinculante 4/2022 sobre la disputa presentada por la Autoridad Irlandesa de protección de datos sobre Meta Platforms Ireland Limited y su servicio Instagram (art. 65 del RGPD).

Los argumentos principales esgrimidos por Meta fueron los siguientes: *a)* la publicidad es un servicio esencial (*core service*) de Instagram; *b)* los servicios de Instagram se ofrecen como una experiencia *personalizada*, experiencia que incluye la publicidad comportamental; *c)* la necesidad de dicho tratamiento para la ejecución del contrato estaba claramente indicada en los términos y condiciones; y *d)* el sujeto de datos podía razonablemente esperar el tratamiento de sus datos con tales fines, ya que el servicio se ofrece bajo el lema «Conectándote con marcas, productos y servicios de la manera que te interesa». En líneas generales, la posición de Meta se basaba en afirmar que la actividad de red social y de publicidad en Instagram son prestaciones indisolubles y ambas deben ser personalizadas para ofrecer un mejor servicio al usuario. Además, la publicidad resulta crítica para mantener la rentabilidad del modelo de negocio de Instagram[72].

Desde la óptica de la protección de datos, aceptar que la publicidad (en cualquiera de sus modalidades) y el servicio principal son servicios indisolubles supondría admitir la validez de bases legales como la necesidad para el cumplimiento del contrato o el interés legítimo[73]. Esta aceptación tendría como beneficio para el prestador del servicio poder acudir a bases distintas del consentimiento, lo cual supondría evitar los altos estándares que se aplican bajo la normativa actual para que el consentimiento sea válido. Dicho de otra forma, sostener que la publicidad y el servicio principal son servicios inseparables tendría como beneficio aplicar bases de tratamiento menos exigentes que el consentimiento. Un claro ejemplo de las dificultades que rodean al consentimiento como base de tratamiento con fines publicitarios sería el conocido caso del *pay-or-okay*[74].

Otra de las ventajas de considerar la publicidad y el servicio principal como servicios indivisibles es que permitiría evitar la aplicación de ciertas normas de la DSA cuando el servicio principal no sea una plataforma en el sentido de la norma. En otras palabras, si consideramos que el servicio principal no puede ser separado del servicio de publicidad, cuando el primero no sea un servicio de plataforma no se someterá a las obligaciones de la DSA. Algunos autores señalan, a título de ejemplo, que servicios como los periódicos en línea no son servicios de plataforma, ya que la concurrencia de un control

---

[72] Tales argumentos fueron rechazados en la citada decisión vinculante del CEPD.

[73] Arts. 6 (1) *b)* y *f)* RGDP.

[74] Sánchez Frías, I. «La prohibición de presentar publicidad basada en perfiles utilizando categorías especiales de datos en la Ley de Servicios Digitales. ¿A quién deja atrás? Especial referencia al dilema *pay-or-okay*», *Actas de derecho industrial y derecho de autor*, tomo 44, 2024, pp. 436-437.

o responsabilidad editorial por el propio prestador elimina su carácter de servicio intermediario[75].

Bajo esta perspectiva unitaria, la prohibición de la DSA presentaría grandes lagunas. Algunos autores señalan que esta interpretación no resulta aplicable a los servicios que incorporan anuncios de Google Ads, entendiendo que la prohibición solo se aplica a los anuncios presentados a los propios usuarios de la plataforma[76]. Si, por ejemplo, un periódico *online* inserta en su interfaz anuncios gestionados por Google Ads, bajo una perspectiva unitaria la prohibición no operaría sobre estos anuncios ya que se destinan a los usuarios del periódico *online*. Este planteamiento, como analizaremos a continuación, no nos parece convincente, pues el hecho de que los destinatarios de Google Ads y los usuarios del servicio principal coincidan no es un motivo de exclusión previsto por la norma.

2. Perspectivas delimitadoras. Indicadores a favor de delimitar el servicio principal y el servicio de publicidad

2.1. *La DMA y la regulación de los «servicios integrados»*

Pese a los argumentos esgrimidos por los prestadores de servicios de plataforma para considerar la publicidad inserta en la interfaz del servicio principal como un servicio indisoluble, tanto la DMA y la DSA como las instituciones europeas parecen más tendentes a optar por una delimitación de tales servicios cuando sea posible. Comenzando por la DMA, al designar a los guardianes de acceso, la Comisión debe también indicar qué servicios básicos de plataforma presta cada uno. Hasta la fecha, la Comisión ha designado tres servicios de publicidad como servicios básicos de plataforma[77].

El primero es Amazon Advertising. El propio Amazon ha descrito este como un servicio que permite a los usuarios profesionales publicitar sus productos y servicios en Amazon Marketplace y, en menor medida, en dispositivos y servicios de entretenimiento propiedad de Amazon (por ejemplo, el servicio de plataforma de intercambio

---

[75] Husovec, M. «Principles», en *Principles of the Digital Services Act,* Oxford Academic, 2024, versión *online*.

[76] Becker, S. y Penfrat, J. «The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful», en Van Hoboken, J. *et al.* (ed.) *Putting the Digital Services Act into Practice. Enforcement, Access to Justice, and Global Implications*, Verfassungsbooks, 2023, pp. 53-62.

[77] El art. 2(2) DMA señala que los servicios de publicidad en línea incluyen 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 demás servicios básicos de plataforma.

de vídeos Twitch o su servicio de reproducción de contenido en streaming Prime Video), así como en sitios web y aplicaciones de software de terceros[78]. Contrariamente a las alegaciones de Amazon, la Comisión entendió que Amazon Marketplace y Amazon Advertising son servicios básicos de plataforma diferentes, independientemente del hecho de que ambos se presten, hasta cierto punto, de manera integrada.

Los argumentos de la Comisión para sostener esta conclusión son principalmente dos. El primero es la distinta categorización de ambos servicios. La sección D (2) (c) (i) del anexo de la DMA señala que la empresa prestadora de servicios básicos de plataforma considerará diferentes aquellos servicios básicos de plataforma que la empresa ofrezca de forma integrada pero no pertenezcan a la misma categoría de conformidad con el art. 2.2 de la DMA. Es decir, aunque se presten de forma integrada, el servicio de Marketplace y el servicio de publicidad de Amazon pertenecen a distintas categorías bajo el art. 2.2, por lo que a tenor de la norma constituirían servicios diferenciados. El segundo argumento se basa en la extensión del servicio más allá del servicio de Marketplace de Amazon. Como admitió la propia empresa, Amazon Advertising no se presta exclusivamente a los terceros que ofertan sus productos a través de Amazon Marketplace, sino que el servicio se extiende a otros servicios de Amazon (como Twitch), a páginas web de terceros y a aplicaciones de *software*. Igualmente, la Comisión destacó que, aunque Amazon solo prestase tal servicio a sus propios usuarios profesionales, el mismo seguiría siendo un servicio diferenciado debido a su distinta categorización bajo la DMA.

El segundo servicio de publicidad designado como servicio básico de plataforma es Alphabet's Online Advertising (publicidad digital de Alphabet)[79]. Este caso planteó un desacuerdo diferente, ya que

---

[78] Amazon explica que Amazon Advertising incluye la siguiente variedad de servicios: «(i) "Anuncios patrocinados"; (ii) la plataforma del lado de la demanda de Amazon para la colocación de anuncios en servicios propiedad de Amazon y operados por Amazon, así como en sitios web y aplicaciones de terceros; (iii) "Amazon Publisher Services"; y (iv) "Amazon Ad Server". Amazon explica que Amazon Advertising también incluye "Amazon Attribution" y "Amazon Marketing Cloud", herramientas que los anunciantes que utilizan Amazon Advertising pueden utilizar para medir la eficacia de sus campañas publicitarias».

Vid. Caso DMA.100016 *Amazon – online advertising services*, p. 12 ss.

[79] Conforme a las alegaciones de Alphabet, dichos servicios comprenden una gran variedad de herramientas o servicios, incluyendo a servicios de compra (dirigidos a anunciantes), venta (dirigidos a publicistas) y servicios de intermediación (intermediación entre anunciantes y publicistas, así como otros proveedores de servicios de intermediación publicitaria). Los servicios de compra, como Google Ads, Display & Video 360 («DV360»), Search Ads 360 y Campaign Manager 360, permiten a los anunciantes configurar campañas publicitarias para comprar espacios publicitarios en los servicios y productos de Alphabet (por ejemplo, Search, Maps, Play), así como en propiedades de terceros, incluyendo estos servicios la optimización y medición del rendimiento de los anuncios. Los servicios de venta, como Google Ad Manager, AdSense y AdMob, permiten a los editores vender su espacio publicitario a los anunciantes.

Alphabet no negaba la prestación de servicios de publicidad como un servicio diferenciado. La única divergencia fue en torno a los servicios Google Analytics y AdSense for Search. Aunque Alphabet sostuvo que constituían servicios diferentes a los servicios de publicidad digital (probablemente con el objeto de evadir los umbrales de la DMA), la Comisión concluyó que ambos estaban amparados en el bloque o servicio único de servicios de publicidad digital.

El tercer servicio de publicidad digital designado como servicio básico de plataforma es Meta Ads[80]. Meta cerró filas con posturas que ya había mostrado anteriormente, defendiendo que sus servicios publicitarios «conforman un solo servicio digital de red social sustentado por la publicidad, que engloba a Facebook, Instagram, Meta Ads, Messenger, Marketplace, Facebook Dating y Facebook Gaming Play»[81]. En contra de los argumentos de Meta, la Comisión sostuvo que nos encontramos ante servicios diferenciados, por las mismas razones que en el caso de Amazon Advertising. Es decir, al constituir servicios diferentes conforme al art. 2.2 de la DMA y prestarse incluso en interfaces de terceros, no puede afirmarse que el servicio de publicidad sea indisoluble de los servicios de red social y mucho menos que todos los servicios de Meta conformen un bloque único, independientemente de que la publicidad quede totalmente integrada en otros servicios básicos de plataforma prestados por Meta.

En conclusión, a tenor de la DMA, la postura de la Comisión parece clara. A pesar de que el servicio de publicidad digital pueda quedar integrado en otro servicio básico de plataforma, si la categorización de ambos es distinta nos encontramos ante servicios diferenciados. A estos efectos, será irrelevante si el servicio de publicidad se presta solo a servicios ofrecidos por el mismo guardián de acceso o si también se integra en servicios de terceros.

Vid. Caso DMA.100016 *Amazon – online advertising services*.

[80] Conforme a las alegaciones de Meta, Meta Ads consiste en la interfaz «Ads Manager», que permite a los anunciantes crear, diseñar y administrar sus campañas publicitarias en todo el inventario de Meta, como Facebook e Instagram. Meta también proporciona una extensión de Meta Ads, la «Audience Network», que permite a los anunciantes publicar anuncios en el inventario de aplicaciones móviles de editores externos que forman parte de Audience Network. Por último, Meta explica que Meta Ads incluye «publicaciones promocionadas» (*boosted posts*), así como las funciones de «Tiendas» (*shops*) de Instagram y Facebook. CASO DMA.100035 Meta – online advertising services, p. 24 ss.

[81] Como hemos señalado anteriormente, esta postura tendente a unificar servicios ya había sido mostrada por Meta. Commission decision of 5/9/2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, p.80.

2.2. *La delimitación de los servicios integrados bajo la DSA*

A. La delimitación como garantía del efecto útil

Si bien los objetivos de la DMA y la DSA y sus respectivos conceptos de plataforma son distintos, algunos de estos argumentos son trasladables a la delimitación de servicios de plataforma bajo la DSA. Por un lado, debemos destacar la posibilidad de que los servicios sean delimitables aunque se presten de forma integrada. En otras palabras, la integración de un servicio (la publicidad digital) en otro servicio (el servicio principal) no debería ser un obstáculo para aplicar las normas relativas a las plataformas en línea a ambos servicios si tal diferenciación es posible en un sentido técnico, como bien reconoce el considerando 77 de la DSA. En el mismo sentido se pronunciaban otros autores al señalar que, en ocasiones, los *servicios híbridos* pueden incorporar distintos aspectos que pueden o no ser servicios de plataforma, pero dicha distinción debe hacerse cuando sea posible[82-83].

La separación puede tornarse complicada cuando en un mismo servicio se entremezclan contenidos generados por los usuarios y contenidos presentados por el proveedor bajo su responsabilidad editorial. Recordemos que la DSA solo se aplica a servicios de plataforma en los que la información es generada por los destinatarios, ya sean consumidores (como es el caso de los usuarios de plataformas de citas, como *Tinder*) o usuarios profesionales (como es el caso de las empresas que anuncian servicios turísticos en *Booking*). Se excluyen así aquellos servicios en los que el contenido es generado por la propia plataforma bajo su control editorial (como los servicios de vídeo a demanda o los periódicos *online*)[84].

En Google Maps encontramos un caso particular, ya que el servicio es una combinación entre aportaciones de la empresa y de los usuarios. Sería un ejemplo de servicios indisociables que son regulados en su conjunto como una plataforma que ha sido incluso designada como VLOP[85]. El mismo caso encontramos en algunas webs de contenido sexual, en las que se entremezcla el contenido generado por los usuarios con el contenido seleccionado por el proveedor bajo su responsabilidad editorial. Esta fue una de las razones por la que, en una

---

[82] En adelante, nos referiremos a servicios «híbridos» y servicios «integrados» como conceptos equivalentes.

[83] Husovec, M. «The DSA's Scope Briefly…», *op. cit.*; y Santos, C. *et al.,* «Which Online Platforms and Dark patterns should be regulated under article 25 of the DSA?», 2024.

[84] Husovec, M. «The DSA's Scope Briefly…», *op. cit.*

[85] Commission Decision of 25/4/2023 designating Google Maps as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

segunda ronda de designaciones, la Comisión consideró a Pornhub, XVideos y XNXX como VLOP. La solución generalizada parece ser que cuando los servicios queden técnicamente tan integrados que no se puedan separar, la condición de plataforma se aplicaría al servicio en su conjunto, salvo que el componente de contenido generado por el usuario sea una característica menor y puramente auxiliar.

De forma menos detallada, esta es también la postura que adopta el legislador en el considerando 13 de la DSA. Bajo un lenguaje de difícil inteligencia, se expone el ejemplo de las secciones de comentarios de un periódico en línea, señalando la posibilidad de que se examinen por separado estas secciones y las secciones de noticias a efectos de determinar si el servicio puede ser calificado como plataforma. En caso de que sea una característica menor y puramente auxiliar del servicio principal, no lo calificaría como un servicio de plataforma diferenciado, al quedar englobado en el servicio principal.

Salvando esta postura, parece que la DSA, a diferencia de la DMA, no presta especial atención a la delimitación de los servicios integrados salvo para determinar el número de usuarios activos, cómputo que sirve para identificar cuáles de esos servicios son VLOP[86]. Es decir, la preocupación principal del legislador parece situarse en aquellos casos en los que la separación de los servicios pueda impactar en la designación de las VLOP, ya que deslindar un servicio menor del servicio principal podría causar que este último no alcance los umbrales cuantitativos de usuarios[87]

Aun teniendo este factor en cuenta, la separación de servicios puede tornarse necesaria cuando la integración sea utilizada como mero vehículo para eludir las normas aplicables a las plataformas, situación que iría en contra del efecto útil de la norma, como advierte el considerando 13 de la DSA. Ciertos proveedores, al prestar los servicios de forma integrada, podrían tratar de evadir la aplicación de determinadas obligaciones, como la prohibición de presentar publicidad basada en perfiles usando datos sensibles.

En aras de proteger este efecto útil, la DSA reconoce la posibilidad de que un servicio se preste a través de otro, razonamiento también presente en el anexo de la DMA al referirse a servicios ofrecidos de forma integrada[88]. Conforme al art. 2.2 de la DSA, el Reglamento «no se aplicará a ningún servicio que no sea un servicio intermediario […] con in-

---

[86] El considerando (77) de la DSA señala «(a) fin de determinar el alcance de una determinada plataforma en línea o motor de búsqueda en línea, es necesario establecer el promedio de destinatarios activos de cada servicio individualmente».

[87] Esta es la estrategia que intentaron seguir las plataformas de contenido sexual que fueron designadas en una segunda tanda como VLOPs (Pornhub, XVideos y XNXX).

[88] Así, la sección D (2) (c) (i) del anexo de la DMA señala que la empresa prestadora de servicios básicos de plataforma considerará diferentes aquellos servicios básicos de plataforma

dependencia de si el servicio se presta mediante el uso de un servicio intermediario». Reconoce así que: *a)* un servicio intermediario puede ser el canal de prestación de otro servicio; y *b)* a este otro solo se le aplicará la DSA si también guarda la calificación de servicio intermediario.

En el caso de los servicios de publicidad, cabe asumir que podrán ser reconocidos como servicios de plataforma en línea independientemente de si el servicio principal es o no una plataforma en el sentido de la DSA. Así, por ejemplo, aquellos servicios que no difunden contenido de terceros y que actúan bajo su propia responsabilidad editorial —como los periódicos en línea, o los servicios de vídeo a demanda, como Netflix— o que actúan como mero escaparate, mostrando exclusivamente sus propios productos —como es el caso de Primark— no caerían bajo la denominación de plataformas al no constituir servicios intermediarios. No obstante, si la interfaz de dichos servicios aloja publicidad gestionada, por ejemplo, por Google Ads, deberá analizarse si dicho servicio de publicidad es un servicio de plataforma, independientemente de si el servicio principal es o no una plataforma.

La Comisión Europea parece seguir la misma lógica. En la designación de Facebook como VLOP remarcó que Facebook y Messenger son servicios diferenciados, debiendo caracterizarse solo Facebook como plataforma en línea, ya que Messenger, al tener un número finito de destinatarios, no cumple con el requisito de difundir información al público[89].

B. La delimitación de servicios como factor esencial para la determinación de responsabilidades

Volviendo a posibles aspectos de la DMA que sean trasladables a la delimitación de servicios bajo la DSA, debemos recalcar la importancia de identificar quién es el prestador del servicio de publicidad en cada caso. Aunque la publicidad digital tienda a integrarse en un servicio principal, la gestión de los anuncios es generalmente llevada a cabo por un tercero y no por el proveedor del servicio principal. Esta gestión suele llevarse a cabo por las mismas empresas: Alphabet, Amazon y Meta[90]. Una evidencia de ello es que, bajo la DMA, solo Alphabet's Online Advertising, Amazon Advertising y Meta Ads han sido designados como servicios básicos de plataforma de publicidad,

---

que la empresa ofrezca de forma integrada, pero que no pertenezcan a la misma categoría de servicios básicos de plataforma de conformidad con el art. 2 (2) de la DMA.

[89] Commission Decision of 25/4/2023 designating Facebook as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[90] Cabral, L. *et al.*, *The EU Digital Markets Act…*, *op. cit.*

siendo considerados una puerta de acceso importante para los usuarios profesionales[91].

En aquellos casos en los que la publicidad se inserta en servicios de terceros —es decir, en servicios de proveedores distintos de Alphabet, Amazon o Meta— la labor de este otro proveedor es simplemente habilitar un espacio publicitario en su interfaz, pero es Alphabet, Amazon o Meta quien realiza todas las demás gestiones publicitarias, como la compra y venta de espacios publicitarios, la selección y colocación de anuncios, la determinación algorítmica de los destinatarios, la personalización de los anuncios, la configuración de campañas y las mediciones de eficacia.

Esta diferenciación de papeles es importante a efectos de determinar quién es el responsable de adaptar el algoritmo publicitario para cumplir con la prohibición de presentar publicidad basada en la elaboración de perfiles utilizando datos sensibles. La DSA impone esta prohibición a *los prestadores de plataformas en línea*. Sin embargo, en la publicidad digital personalizada intervienen un gran número de operadores: aquel en cuyo interés se presenta el anuncio, aquel que habilita el espacio publicitario en su interfaz y aquellos que realizan diversos servicios de intermediación, como los anteriormente señalados. Así lo reconoce el considerando 17 de la DSA, al señalar que en la publicidad en línea generalmente intervienen varios actores, incluidos los servicios intermediarios que conectan a los editores con los anunciantes.

En España, el art. 8 de la Ley General de Publicidad clasifica a dichos operadores en tres grupos. En primer lugar, distingue al anunciante, es decir, la persona natural o jurídica en cuyo interés se realiza la publicidad. Pongamos como ejemplo un anuncio en el periódico digital El Mundo sobre un ordenador vendido por MediaMarkt. En este caso, el anunciante sería MediaMarkt, ya que es la empresa en cuyo interés se realiza la publicidad.

En segundo lugar, se encuentran las agencias de publicidad, definidas como aquellas personas naturales o jurídicas que se dediquen profesionalmente y de manera organizada a crear, preparar, programar o ejecutar publicidad por cuenta de un anunciante. Siguiendo el ejemplo anterior, cuando pinchamos en el apartado «ad preferences» del anuncio en cuestión, nos desviará a la página web de Amazon Ads, que es el servicio que gestiona la publicidad inserta en la interfaz de El Mundo. Conforme a esta clasificación, la agencia de publicidad sería Amazon, al ser la encargada de ejecutar la publicidad encargada por el anunciante.

---

[91] Casos DMA.100035 *Meta – online advertising services* y DMA.100016 *Amazon – online advertising services*.

Por último, la norma distingue a los medios de publicidad, definidos como aquellas personas naturales o jurídicas, públicas o privadas, que, de manera habitual y organizada, se dediquen a la difusión de publicidad a través de los soportes o medios de comunicación social cuya titularidad ostenten. Siguiendo el ejemplo anterior, el medio de publicidad sería el periódico El Mundo, cuya titularidad es ostentada por Unidad Editorial S. L. U.[92].

En algunos casos, es posible que varias o todas estas categorías concurran en un mismo actor. Un ejemplo serían los anuncios de terceros insertados en Facebook. Meta ejercería tanto de medio publicitario —al alojar los anuncios en la interfaz de su servicio de red social— como de agencia de publicidad —ya que los anuncios se gestionan a través de Meta Ads—. Otro ejemplo sería la publicidad de productos del propio Amazon vendidos en su Marketplace. En este caso, confluirían en un mismo prestador todos los anteriores roles, ya que el anunciante sería Amazon, las tareas propias de una agencia de publicidad serían desempeñadas a través del sistema Amazon Advertising, y el medio publicitario sería Amazon Marketplace.

Si bien la clasificación de la normativa española puede parecer arcaica o desfasada para las complejidades actuales de la publicidad digital personalizada, sus nociones son claras para delimitar las funciones en la prestación del servicio. Así, en casos en los que interviene una multiplicidad de empresas debemos plantear cuál o cuáles de estos operadores son responsables de ejercer las pertinentes medidas de *compliance* para evitar que la publicidad se base en la elaboración de perfiles usando datos sensibles. Esta prohibición solo se aplica a los prestadores de plataformas en línea, por lo que habrá que determinar quién es el prestador de la actividad prohibida.

Como planteábamos en apartados anteriores, a los que nos remitimos, la norma parece situar el protagonismo en la selección (*targeting*) de un destinatario u otro conforme a datos que sean sensibles. En consecuencia, las obligaciones de *compliance* se situarían en el prestador del servicio de plataforma que realice dicha selección de destinatarios. Siguiendo el hilo anterior, poco sentido tendría responsabilizar al medio publicitario con medidas relativas al diseño del algoritmo, cuando su única labor es ofrecer su interfaz para la presentación de anuncios sin intervenir en la selección de los destinatarios conforme a perfiles elaborados por un tercero. El mismo argumento sería aplicable a los anunciantes cuando la selección dependa del algoritmo publicitario del prestador de los servicios de intermediación (Amazon, Meta o Alphabet).

---

[92] Información facilitada por los Términos y Condiciones de Uso de *El Mundo*, disponibles en *https://www.elmundo.es/registro/avisolegal.html.*

En estos casos, sería el prestador de estos servicios de intermediación publicitaria el responsable de respetar la prohibición y aplicar las principales medidas de *compliance,* ya que es su algoritmo publicitario el que selecciona los anuncios y a sus respectivos destinatarios conforme a los datos a los que tiene acceso. Esta interpretación sería la más coherente, ya que ni el espacio publicitario ni los anunciantes acceden a los datos —sensibles o no sensibles— utilizados para la elaboración de perfiles.

Por otro lado, es la que más garantiza el efecto útil de la norma, ya que el prestador de los elementos principales del servicio de publicidad es el intermediario, no el medio. Si entendiésemos lo contrario, es decir, que el obligado es el medio publicitario, podríamos encontrarnos ante casos en los que el medio que aloja la publicidad no sea una plataforma y, en consecuencia, no se le aplique la prohibición. Esta interpretación carece de sentido, ya que los datos que permiten la elaboración de perfiles son seleccionados y analizados por el algoritmo publicitario del intermediario, que es quien igualmente elabora tales perfiles, y no por el medio publicitario que simplemente ofrece un espacio en su interfaz.

En algunos casos, sin embargo, ciertas características técnicas del medio publicitario pueden ser relevantes ya que pueden afectar a la calificación de la publicidad integrada como servicio de plataforma y, consecuentemente, a la aplicabilidad de la prohibición.

IV. ¿ES SIEMPRE UN SERVICIO INTERMEDIARIO DE PUBLICIDAD EN LÍNEA UN SERVICIO DE PLATAFORMA? POSIBLES EXCEPCIONES BAJO LA DSA

Para que al prestador de los servicios intermediarios de publicidad en línea (al que la normativa española se refiere como agencia de publicidad) se le aplique la prohibición de presentar publicidad basada en perfiles utilizando datos sensibles es preciso determinar si dichos servicios constituyen servicios de plataforma en línea en el sentido de la DSA, que limita a éstos su ámbito subjetivo[93].

Aunque la DSA no establece un listado taxativo de servicios de plataforma en línea, hay ciertos preceptos que hacen alusión a los servicios intermediarios de publicidad, si bien su categorización no resulta del todo clara. A título de ejemplo, el art. 46.1 de la DSA recoge que la Comisión fomentará y facilitará la elaboración de códigos de conducta voluntarios «por prestadores de plataformas en línea y otros prestadores

[93] Art. 26 (3) DSA.

de servicios pertinentes, como los prestadores de servicios intermediarios de publicidad en línea». Cabe plantearnos si la norma, bajo este precepto, está excluyendo a los servicios de intermediación publicitaria de los servicios de plataforma, al considerarlos como *otros servicios pertinentes*, o si esta alusión es meramente complementaria para que el precepto se acomode al principio de neutralidad tecnológica.

La respuesta no es sencilla, aunque inicialmente puedan señalarse dos ideas claras. La primera es la posibilidad de que el servicio de publicidad se segregue del servicio principal en el que está integrado, como veníamos exponiendo en apartados anteriores, que damos por reproducidos. La segunda es la calificación del servicio de intermediación publicitaria como un servicio intermediario regulado bajo la DSA. Como indica Husovec, el almacenamiento de anuncios constituye indiscutiblemente un servicio intermediario de alojamiento[94]. La discusión radica en si dichos servicios encajan dentro de la subcategoría de plataformas en línea. El mismo autor sostiene que si dichos anuncios almacenados son también difundidos al público nos encontramos probablemente ante un servicio de plataforma *online*.

Este *«probablemente*» es muy significativo, ya que nos da a entender que pueden concurrir excepciones. Tales excepciones serían la razón principal por la que la DSA no califica de forma rotunda a todos los servicios intermediarios de publicidad como servicios de plataforma en línea. Planteábamos al finalizar el anterior apartado cómo ciertas características del medio publicitario o servicio principal pueden afectar a la calificación del servicio de publicidad como servicio de plataforma.

Haciendo un breve análisis, para que un servicio *online* sea calificado como plataforma, debe cumplir previamente con una primera capa: ser un servicio de intermediación en el sentido del art. 1.1.*b)* de la Directiva 2015/1535[95][96]. Los servicios de intermediación publicitaria cumplirían con los requisitos del citado precepto, al ser servicios prestados a cambio de una remuneración (ya sea monetaria, ya sea a través de otros medios, como el pago con datos de los usuarios), a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

La segunda capa que debe cumplirse requiere que se trate de un servicio de alojamiento de datos, en el sentido del art. 3.*g)*.iii) DSA. Es decir, el servicio debe consistir en almacenar datos facilitados por el destinatario del servicio y a petición de este. Los datos almacenados

---

[94] Husovec, M. «Principles», *op. cit.*

[95] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo de 9 de septiembre de 2015 por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

[96] Definición por remisión del art. 3 *a)* DSA.

serían los anuncios facilitados por los anunciantes y a petición de estos, los cuales guardan la calificación de destinatarios, ya que la norma ampara como tales a todas las personas físicas o jurídicas que utilicen el servicio de intermediación[97].

La última capa sería que el servicio cumpla con los requisitos para ser considerada plataforma en línea. En este punto, la nota característica que hace que un servicio de alojamiento sea también una plataforma es la difusión de información al público, requisito que, como planteábamos en un anterior apartado, puede resultar problemático al excluir a aquellos servicios que presenten un número limitado de destinatarios. Aunque el servicio de publicidad se preste de forma integrada en el servicio principal, hemos planteado anteriormente que existe una tendencia a separar ambos servicios cuando sea técnicamente posible. Sin embargo, el establecimiento de un número limitado de destinatarios supondrá no solo la exclusión del servicio principal como un servicio de plataforma, sino también del servicio de publicidad alojado en la interfaz del servicio principal.

En otras palabras, por regla general el servicio principal puede ser delimitable del servicio de publicidad, aunque ambos se presenten de forma integrada. Un ejemplo sería la publicidad inserta en los periódicos *online* o en los servicios de vídeo a demanda. Sin embargo, cuando el servicio principal (el medio publicitario) presente un límite técnico de destinatarios, este límite técnico afectaría no solo al servicio principal, sino también al servicio de publicidad. Este sería el caso de la publicidad inserta en mensajes de Telegram y Gmail, ya que ambos presentan un número finito de destinatarios. En este tipo de publicidad, la prohibición de la DSA no operaría, ya que no nos encontraríamos ante un servicio publicitario de plataforma, al no difundir información al público en el sentido de la DSA.

El segundo punto que puede generar dudas aplicativas es la exclusión del concepto de plataforma de aquellos servicios en los que la difusión «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 […] Reglamento». En consecuencia, habrá que realizar un análisis casuístico de tres factores.

El primero es si la difusión al público (es decir, la difusión de publicidad) es una característica menor y puramente auxiliar del servicio principal. La norma no ofrece indicadores de cuándo se da esta situación, si bien un indicador económico podría ser el nivel de ingresos

[97] Art. 3 *a)* DSA.

que percibe el servicio principal como consecuencia de la publicidad. Otros parámetros desde una perspectiva de aproximación por riesgo (que es la que impera en la DSA) serían el número de destinatarios de dicha publicidad y la cantidad de anuncios que aloja la interfaz. Por regla general, cuando el servicio principal base su modelo de negocio en la publicidad (como es el caso de los periódicos *online*) será difícil sostener que la publicidad es un servicio menor. Mayores interrogantes pueden plantearse en aquellos servicios que no son de plataforma y combinan ingresos publicitarios con las tasas de suscripción de los usuarios, como es el caso de algunas tarifas de Netflix. En otras palabras, habría que determinar caso por caso si la publicidad es una funcionalidad menor y puramente auxiliar del servicio principal.

Para que aplique esta exclusión, solo en aquellos casos en los que la publicidad sea una característica menor tendrá que analizarse un segundo elemento: que la publicidad en cuestión no pueda utilizarse sin ese otro servicio principal por razones objetivas y técnicas. En este punto puede resultar discutible si la publicidad basada en perfiles puede presentarse sin estar integrada en cierto modo en otro servicio. Aunque es cierto que *offline* la publicidad puede no estar integrada en otros servicios (como es el caso del reparto de folletos), en la publicidad *online* dicha integración es necesaria. Ahora bien, reiteramos que este examen solo es necesario cuando la publicidad sea una característica menor y puramente auxiliar del servicio principal. El precepto finaliza incluyendo una cláusula de seguridad o de cierre, al señalar que esta exclusión no operará cuando la integración sea un mero medio para eludir la aplicabilidad de la DSA. Esta última referencia se formula como una vía para que aquellos servicios de publicidad que planteen riesgos significativos no queden fuera del ámbito de aplicación de la norma.

Concluyendo, podemos destacar que no en todos los casos un servicio intermediario de publicidad será una plataforma en línea en el sentido de la DSA. Se excluyen aquellos servicios de publicidad integrados en un servicio principal que tenga un número finito de destinatarios, así como aquellos en los que la difusión de publicidad sea una característica indudablemente menor y auxiliar del servicio principal. Sin embargo, en aquellos servicios cuyo modelo de negocio se base en la publicidad, será más defendible la calificación como plataforma en línea y la aplicación de las normas relativas a estas.

Para buscar el efecto útil de la norma y evitar posibles fraudes de ley, dichas excepciones deberían aplicarse con cautela, ya que la DSA no solo prohíbe la publicidad basada en perfiles usando datos sensibles, sino que también presenta otros objetivos, como la lucha contra la difusión de contenidos ilícitos, por ejemplo, la publicidad sobre productos que infrinjan derechos de propiedad intelectual e in-

dustrial[98]. Dicho de otra forma, una excesiva aplicación de las excepciones expuestas reduciría la eficacia de la DSA, ya que la mayoría de las obligaciones se sitúan en las plataformas en línea, y los servicios de intermediación publicitaria plantean un gran número de riesgos sistémicos que la norma pretende paliar al regular la actividad de dichas plataformas[99].

V. ¿DEBERÍAN LOS GRANDES SERVICIOS DE INTERMEDIACIÓN PUBLICITARIA (ALPHABET ADVERTISING, META ADS Y AMAZON ADS) SER DESIGNADOS COMO VLOPS?

Anteriormente, señalábamos que la gran mayoría de los servicios de intermediación publicitaria *online* son prestados por un oligopolio de empresas: Alphabet —a través de Alphabet Advertising Services—, Meta —a través de Meta Ads— y Amazon —a través de Amazon Ads—. En caso de que estos servicios sean delimitables del servicio principal en el que quedan integrados y no opere ninguna de las excepciones que hemos expuesto, cabría plantearnos si dichos servicios cumplen con los requisitos para ser designados por la Comisión como VLOPs (designación que, hasta la fecha, no se ha producido).

Al igual que en el caso de los guardianes de acceso, bajo la DSA la designación de VLOPs por parte de la Comisión tiene carácter constitutivo. Es decir, las obligaciones aplicables a las VLOPs solo se imponen a la plataforma en cuestión una vez que la misma es designada por la Comisión, si bien se establece un periodo de transición de 4 meses desde la notificación de la decisión para que el cumplimiento de las obligaciones sea exigible[100]. Para ser designada como VLOP, la plataforma en cuestión debe alcanzar o superar el promedio mensual de 45 millones de usuarios activos en la UE, que debe calcularse conforme al promedio de los seis últimos meses[101].

---

[98] A título de ejemplo, el informe de transparencia bianual de Google sobre sus VLOP/VLOSE señala que una gran mayoría de acciones emprendidas por Google se destinan a paliar los contenidos ilícitos por infracción de normativa sobre propiedad intelectual (entendida esta en sentido amplio, englobando tanto la propiedad intelectual como industrial). En el caso de Google Search, la empresa tomó un número de 8 948 767 acciones para combatir infracciones de propiedad intelectual tan solo entre el 11 de septiembre de 2023 y el 29 de febrero de 2024. *Vid. Informe de transparencia de Google*, disponible en *https://transparencyreport.google.com/report-downloads?hl=en_GB*.

[99] A título de ejemplo, el considerando (84) de la DSA señala que las evaluaciones de riesgos sistémicos deben centrarse, en particular, en los sistemas algorítmicos de los sistemas de recomendación y publicidad, dedicando especial atención a las prácticas conexas de recogida y uso de datos.

[100] Art. 33 (6) DSA.

[101] Arts. 24 (2) y 33 (1) DSA.

Es reseñable que la norma exige que dicho umbral cuantitativo sea alcanzado computando solo los destinatarios *activos*. Conforme al art. 3 *p)* de la DSA, son destinatarios activos aquellos que hayan utilizado una plataforma, bien solicitando a la plataforma que aloje información, bien exponiéndose a la información alojada en la plataforma y difundida a través de su interfaz[102].

Si bien el término interfaz suele asociarse comúnmente a una página web, el art. 3.*m)* de la DSA entiende este término de una forma más amplia, al definirlo como «todo programa informático, incluidos los sitios web o partes de sitios web, y las aplicaciones, incluidas las aplicaciones móviles». Siguiendo esta definición, el término interfaz incluye aquel programa o algoritmo utilizado para seleccionar la publicidad. Por tanto, el prestador del servicio de publicidad está difundiendo la misma *a través de su interfaz*, ya que es su programa informático el que gestiona la sección de publicidad, independientemente de que los anuncios se integren en el sitio web del servicio principal. De haber optado por una definición menos tecnológicamente neutra, se estaría excluyendo la posibilidad de que los servicios publicitarios de plataforma que hacen uso de webs de terceros pudieran ser designados como VLOPs, exclusión que sería incoherente con la norma, ya que muchas de las obligaciones de las VLOPs se centran en requisitos de transparencia aplicables a la publicidad en línea.

Retornando al concepto de destinatarios activos, leyendo en conjunto los apartados *p)* y *b)* del art. 3, se deduce que los mismos incluyen tanto a los destinatarios profesionales como a los consumidores y usuarios[103]. Esta misma aclaración es ofrecida por la Guía facilitada por la Comisión para el recuento de destinatarios activos, la cual indica que debe incluirse en la contabilización a los consumidores, los usuarios profesionales y los comerciantes[104]. Algunos autores simplifican todavía más este término, al señalar que son destinatarios activos aquellos que, bien crean contenido o bien lo consumen[105]. En el caso de los servicios de intermediación publicitaria, deberían por tanto computarse como destinatarios activos los anunciantes que hacen uso del servicio de intermediación publicitaria, los medios publicitarios que alojan

---

[102] La definición de destinatarios activos es sensiblemente diferente para las plataformas y para los motores de búsqueda. Mientras que en las plataformas la mera exposición o difusión de contenido constituye una participación activa, en los motores de búsqueda la única nota definitoria es la realización de una búsqueda, lo que lleva a excluir del concepto a aquellos destinatarios que utilicen el motor de búsqueda para ofrecer sus productos o servicios, como señala el considerando (77) de la DSA.

[103] El art. 3 *b)* define al destinatario del servicio como «toda persona física o jurídica que utilice un servicio intermediario, en particular para buscar información o para hacerla accesible».

[104] European Commission, «DSA: Guidance on the requirement to publish user numbers», 2023.

[105] Husovec, M. y Roche Laguna, I. «Digital Services Act…», *op. cit.*

dicha publicidad y los usuarios finales (sean o no consumidores y usuarios) del medio publicitario.

Sin embargo, en este último grupo de usuarios finales se puede plantear la duda de cuándo nos encontramos ante destinatarios activos. El término *activo*, conforme a la definición de la RAE, denota cierta tendencia a tomar una iniciativa, factor que podría ser discutible cuando el destinatario es meramente expuesto a un anuncio. La respuesta que otorgan tanto el considerando 77 como la Guía parece ser que la mera exposición es suficiente, al señalar que son destinatarios activos aquellos expuestos a información, por ejemplo, viéndola o escuchándola; no estando limitada la participación activa «a interactuar con la información pulsando, comentando, enlazando, compartiendo, comprando o realizando transacciones». Siguiendo esta lógica, resultaría suficiente la mera exposición al anuncio, por ejemplo, haciendo *scroll* entre los contenidos, sin necesidad de que el destinatario haga clic en el anuncio o llegue a adquirir el producto o servicio publicitado.

Por lo que atañe al recuento de los destinatarios en el caso de los servicios de plataforma de intermediación publicitaria, este resultaría del sumatorio de tres tipos de destinatarios. El primer tipo se compone de los anunciantes que hacen uso del servicio de intermediación publicitaria, considerados destinatarios activos al facilitar el contenido difundido por el servicio de intermediación. El segundo estaría conformado por los usuarios finales que son expuestos a la publicidad. El tercero se integraría por los medios publicitarios de los que el servicio de intermediación se vale para difundir la publicidad, es decir, aquellos servicios principales en los que se inserta la publicidad, como las redes sociales, los periódicos en línea, los marketplaces o las webs de mero escaparate. En estos casos, si bien nos encontramos ante servicios diferenciados (el servicio principal y el servicio de publicidad), el número de destinatarios de ambos sería el mismo cuando el acceso al servicio principal suponga la exposición imperativa al servicio de publicidad.

Ahora bien, existe una relevante excepción a esta norma general. En caso de que el servicio principal ofrezca alternativas sin publicidad (como es el caso de algunos periódicos digitales), entendemos que el cómputo de destinatarios del servicio de intermediación publicitaria debería limitarse a los destinatarios activos de la modalidad con publicidad. A estos efectos, habría que computar solo los usuarios que han accedido al menos una vez en los últimos seis meses a la alternativa ofrecida con publicidad[106]. Esta excepción sería útil para calcular el número real de destinatarios, si bien la norma no prohíbe un ex-

[106] Conforme indican el art. 24 (2) y el considerando (77) de la DSA, el promedio de destinatarios activos de plataformas debe medirse teniendo en cuenta los destinatarios que hayan accedido al menos una vez al servicio en un periodo de referencia de 6 meses para la publicación de los respectivos informes sobre destinatarios activos.

ceso de cómputo de destinatarios, como señala Husovec[107]. En otras palabras, la norma solo exige que la plataforma no declare un número de destinatarios activos inferior al real, pero nada impide que se declare un número superior. Un indicador de esta permisibilidad de cómputo excesivo es que tanto el considerando 77 como la guía aclaran que las plataformas *podrán* descontar del cómputo a los usuarios automatizados, como los *bots* o los extractores de información si disponen de los medios técnicos necesarios, pero no tienen la obligación de realizar este descuento.

Como señalábamos al iniciar este apartado, los principales intermediadores publicitarios en el mercado digital son Alphabet, Amazon y Meta. Se trata de prestadores que ofrecen una multiplicidad de servicios diferentes a la intermediación publicitaria. El considerando 77 de la DSA aclara que el examen para determinar los destinatarios activos debe realizarse respecto de cada servicio individualmente. Pero, hasta la fecha, ninguno de estos prestadores ha informado del número de destinatarios activos de sus servicios de intermediación publicitaria.

En febrero de 2023 Alphabet publicó un informe con el número de destinatarios activos de muchos de sus servicios, como Google Search, Google Maps, Google Play y YouTube, pero sin distinguir su servicio de intermediación publicitaria como un servicio diferenciado[108]. En el informe de transparencia de Google de abril de 2024, informó sobre las medidas adoptadas para cumplir con las normas relativas a la publicidad inserta en los servicios anteriores, pero tratándola como un servicio no diferenciable del servicio principal[109]. Los informes presentan ciertas dicotomías. Por un lado, el informe sobre el número de destinatarios activos no deslinda entre el servicio de publicidad y el resto de servicios. Por otro lado, el informe de transparencia reconoce que la publicidad de Google se inserta en múltiples VLOPs y VLOSEs, estando la revisión de tales anuncios sometida a las políticas de Google Ads[110]. El establecimiento de una política concreta para los anuncios de Google, diferenciable de las políticas de otros servicios (como Google Maps), puede dar a entender que es un servicio diferenciable, si bien esta diferenciación no se da en el cómputo de destinatarios activos.

Meta también publicó un informe sobre sus destinatarios activos en 2024. Este informe fue mucho menos exhaustivo que el de Alphabet, ya que solo incluyó información sobre los servicios que consideraba

---

[107] Husovec, M. y Roche Laguna, I. «Digital Services Act…», *op. cit.*

[108] Google, «Information about Monthly Active Recipients under the Digital Services Act (EU)», 16 February 2023.

[109] Google, «EU Digital Services Act (EU DSA) Biannual VLOSE/VLOP Transparency Report», 26 April 2024.

[110] *Ibid.*, p. 23.

que alcanzaban los umbrales: Facebook e Instagram[111]. Hasta la fecha, solo estos dos servicios han sido designados como VLOPs. Es reseñable que en el informe sobre transparencia que publicó en abril de 2024 siguiese sin diferenciar a su servicio de intermediación publicitaria como un servicio diferenciable de Facebook e Instagram pero, aun así, hiciese múltiples referencias a la política publicitaria *(Advertising Standards)* de Meta[112]. Al igual que en el caso de Google Ads, la política seguida es común a todos los servicios de intermediación publicitaria que presta la empresa.

El 17 de febrero de 2023 Amazon publicó un informe en el que declaraba que solo Amazon Store cumplía con los umbrales para ser designado como VLOP. En consecuencia, hasta la fecha, este ha sido el único servicio de la empresa designado como tal[113]. En el informe de transparencia que emitió en abril de 2024 encontramos la misma lógica que en los informes de Meta y Alphabet: no se reconoce al servicio de intermediación publicitaria como un servicio diferenciado, pero sí se hacen múltiples referencias a la política publicitaria (Ad Policies) de Amazon, que es aplicable tanto a los anuncios insertados en Amazon Store como a otros servicios del prestador y de terceros[114].

Pese a que ninguna de las empresas que controla el mercado digital de la intermediación publicitaria haya reconocido sus servicios publicitarios como un servicio diferenciado en los informes de transparencia sobre destinatarios activos, debemos destacar que dichos informes no son vinculantes para la Comisión. Así, el art. 33.4 de la DSA contempla que la Comisión puede basar su decisión no solo en la información facilitada por el prestador o en la información solicitada, sino también en cualquier información de la que disponga. Este fue el procedimiento seguido en la segunda ronda de designaciones, en la que la Comisión atribuyó esa consideración a Pornhub, Stripchat y XVideos no con base a la información facilitada por los prestadores, sino tras un proceso de investigaciones iniciado *ex officio*[115].

Por lo que respecta a los servicios de intermediación publicitaria de Alphabet, Meta y Amazon, se podrían seguir varios procedimientos. Por un lado, la Comisión podría solicitar a dichos prestadores que ofrezcan información más detallada sobre el número de destinatarios activos del servicio. Por otro, independientemente de que esta

---

[111] Meta, «Digital Services Act – Information on Average Monthly Active Recipients in the European Union», 14 de febrero de 2023.

[112] Meta, «Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Facebook», 16 de abril de 2024.

[113] Commission Decision of 25/4/2023 designating Amazon Store as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[114] Amazon, «EU Store Transparency Report», abril de 2024.

[115] European Commission, «Commission designates second…», *op. cit.*

información se facilite o no, la Comisión también podría iniciar investigaciones independientes o hacer uso de información de la que ya disponga de cara a discernir si se cumple o no el presupuesto de hecho. Entre esta información podría usar los informes aportados por las empresas en otros contextos como, por ejemplo, en la designación de guardianes de acceso. Igualmente, también resulta relevante el número de destinatarios activos que han declarado dichos prestadores para otros servicios que sí se han reconocido como VLOP. Anteriormente exponíamos que el número de destinatarios activos de un servicio principal que integre publicidad coincidirá con el número de destinatarios activos del servicio de publicidad, ya que para que el destinatario sea considerado como activo solo se exige que sea expuesto al anuncio.

Trasladando este hilo argumental, si Facebook e Instagram alcanzan los niveles cuantitativos, es razonable afirmar que Meta Ads lo alcanzaría también, ya que su número de destinatarios activos abarca no solo la suma de los destinatarios activos de estas redes sociales, sino también de otros medios donde inserte la publicidad y el número de anunciantes que contraten sus servicios de intermediación publicitaria. Lo mismo sucedería en el caso de Amazon Ads, ya que Amazon Store alcanza los umbrales mínimos de destinatarios activos; y con el servicio de publicidad de Alphabet, utilizado en los diversos servicios de la compañía que han sido designados como VLOP (como Google Play, Google Maps o YouTube).

Concluyendo, la ventaja de esta designación radicaría en que los anuncios que presenten quedarían sometidos a las normas de las VLOP no solo cuando se inserten en la interfaz de otra VLOP, sino también cuando se inserten en otros servicios *online* que difundan información al público, aunque estos no hayan sido designados como VLOP.

VI. MEDIDAS DE COMPLIANCE A EJECUTAR POR CADA PRESTADOR IMPLICADO EN SERVICIOS QUE INTEGREN PUBLICIDAD *ONLINE* BASADA EN PERFILES

En la práctica, resulta fundamental determinar qué prestador queda obligado a ejecutar cada medida de cumplimiento con las obligaciones impuestas por la norma (*compliance*) en relación con la presentación de publicidad *online* basada en perfiles. Cuando en un mismo prestador concurran todos los roles —anunciante, medio publicitario y agencia publicitaria—, este asumirá todas las obligaciones relativas a adoptar medidas *ex ante*. Sería el caso de productos de Alphabet (anunciante) que son anunciados en su servicio Google Shopping (medio publicitario) utilizando el sistema publicitario de Google Ads (servicio de agencia o de intermediación publicitaria). En cambio, cuando estos

papeles sean desempeñados por prestadores distintos, la distribución de las obligaciones puede tornarse más complicada.

En este punto, hay que distinguir dos tipos de medidas de *compliance*. El primer conjunto lo conforman las medidas para entrenar y adaptar el sistema de IA empleado, de forma que no seleccione a los destinatarios conforme a perfiles basados en datos sensibles ni personalice el contenido de la publicidad conforme a datos sensibles. El segundo tipo lo conforman las medidas de transparencia respecto a los parámetros seguidos.

Respecto al primer tipo de medidas, siendo el sistema de IA del servicio de intermediación publicitaria el que analiza los datos, elabora los perfiles y, en suma, determina la publicidad que recibe cada destinatario, lo razonable sería afirmar que la obligación de entrenar y adaptar el sistema de IA para que no utilice datos sensibles con fines de publicidad basada en perfiles recae sobre el prestador del servicio de intermediación publicitaria.

Esta interpretación solo opera si entendemos que el servicio de intermediación publicitaria es una plataforma en línea, ya que la prohibición recae sobre los prestadores de plataformas. Si entendiésemos que el servicio de publicidad no es escindible del servicio principal en el que se integra, sería el prestador del servicio principal de plataforma el encargado de velar por que la prohibición se cumpla, sin perjuicio de que posteriormente pueda ejercer su derecho de repetición contra el prestador del servicio de intermediación publicitaria por responsabilidades derivadas del incumplimiento de la prohibición.

La implementación técnica de estas medidas en el algoritmo o sistema de IA utilizado con fines publicitarios se enfrentará al desafío que llevamos planteando a lo largo de este trabajo: la trazabilidad del proceso seguido por el sistema de IA y la determinación de qué datos personales son sensibles, tarea que se torna especialmente ardua cuando se utilizan como inputs *proxies* y datos inferidos, cuya calificación como datos sensibles conforme al RGPD no siempre resulta clara.

A la hora de discernir quién asume las obligaciones relativas a la transparencia sobre los parámetros utilizados, debemos partir de una diferencia importante. El art. 26.3 DSA impone *a los prestadores de plataformas en línea* la prohibición de presentar publicidad basada en perfiles usando datos sensibles, pero no exige que la publicidad se presente en una interfaz de ese prestador para que la prohibición resulte aplicable. Es decir, la prohibición se extiende también a publicidad incluida en interfaces de terceros, factor que permite sostener que el servicio de publicidad es un servicio diferenciable del servicio principal y que las obligaciones de *compliance* de cada uno de los prestadores son distintas.

En cambio, el mismo art. 26, en su apartado primero, establece ciertas obligaciones para los prestadores de plataformas en línea que presenten anuncios publicitarios en sus interfaces en línea. La formulación del precepto exige, a diferencia de en el precepto anterior, que la publicidad se inserte en la interfaz del prestador de la plataforma. Por tanto, será el prestador del servicio principal de plataforma que aloje el anuncio el que deba hacer frente a las obligaciones de transparencia del art. 26.1.

Este precepto obliga al prestador a que se asegure de que, por cada anuncio publicitario concreto presentado a cada destinatario específico, los destinatarios del servicio sean capaces de identificar, de manera clara, concisa e inequívoca y en tiempo real, lo siguiente:

> 1) Que la información es un anuncio publicitario, en particular mediante indicaciones destacadas, que podrían seguir determinadas normas de elaboración y aplicación voluntarias (en virtud del art. 44 DSA).

El requisito de identificar la publicidad como tal no es nuevo en la normativa de la UE ni en la española[116]. El art. 7 de la DPCD califica como omisión engañosa no dar a conocer el propósito comercial de la práctica cuando no resulte evidente por el contexto. Igualmente, el art. 9 de la LGP impone a los anunciantes la obligación de desvelar inequívocamente el carácter publicitario de sus anuncios.

Uno de los principales riesgos de esta omisión es la concurrencia de la denominada publicidad encubierta, es decir, aquella publicidad no identificable como tal por el destinatario[117]. En la publicidad encubierta la naturaleza y el propósito publicitario de un mensaje se disfrazan u ocultan bajo la apariencia de un mensaje informativo o de otra naturaleza, atribuyéndole un valor superior al que tendría si el destinatario conociese su propósito publicitario[118]. En España, como señalan algunos autores, la publicidad encubierta sufre una suerte de multiplicidad regulatoria bajo la LCD: como acto de engaño bajo el art. 7,

---

[116] Peinado Gracia, J. I. «La publicidad desleal: aproximación a la publicidad comparativa en su proyectada regulación en la Unión Europea», en *La constitución española en el ordenamiento comunitario europeo (III): XVIII jornadas de estudio*, 1999, pp. 565-612; Tato Plaza, A. «La reforma de la Ley General de Publicidad», *Revista de derecho de la competencia y la distribución*, núm. 7, 2010, pp. 141-154; Tato Plaza, A. «Obligaciones específicas de información, engaño por omisión y principio de integridad de la campaña publicitaria», en *Actas de derecho industrial y derecho de autor*, tomo 38, 2017-2018, pp. 183-205; Lema Devesa, C. y Fernández Carballo-Calero, P. «Las prácticas publicitarias engañosas en la Directiva de 11 de mayo de 2005», en *Comunicaciones en propiedad industrial y derecho de la competencia*, núm. 46, 2007, pp. 77-90.

[117] Fernández Nóvoa, C., «La publicidad encubierta», en *Estudios de Derecho de la Publicidad*, Universidad de Santiago de Compostela, 1989, pp. 189ss.

[118] Tato Plaza, A. «Aspectos jurídicos de la publicidad a través de líderes de opinión en redes sociales ("influencers")», *Revista de Derecho Mercantil*, 2019, pp.3-6.

como omisión engañosa en el art. 5, y como un supuesto específico de práctica engañosa con los consumidores en el art. 26[119].

Esta obligación ha dado lugar a que plataformas como Instagram o Facebook hayan adaptado progresivamente sus interfaces y activado una opción para que los usuarios marquen ciertas publicaciones con términos como «anuncio», «contenido patrocinado» o «publicidad».

De todas las obligaciones de transparencia, esta es quizás la más reseñable por su novedad y complejidad. Hasta ahora no se venía exigiendo que los prestadores facilitasen en su interfaz información acerca de los parámetros utilizados para seleccionar a los destinatarios de cada anuncio en concreto. Esta nueva inclusión obedece a la creciente tensión en la UE por el uso de técnicas de segmentación optimizadas para responder a los intereses de los destinatarios y apelar potencialmente a sus vulnerabilidades, pudiendo entrañar efectos negativos especialmente graves[120].

El considerando 68 es el encargado de desarrollar este requisito, señalando que la información sobre los parámetros debe ofrecer explicaciones útiles sobre la lógica utilizada para seleccionar a los destinatarios. Indica que dichas explicaciones deben incluir información sobre el método utilizado para presentar el anuncio publicitario, por ejemplo, si se trata de publicidad contextual o de otro tipo y, en su caso, los principales criterios empleados para la elaboración de perfiles. Algunos autores señalan que dichas explicaciones deben ser sencillas y claras para el destinatario para resultar útiles, por lo que no es necesario que desvelen con detalle procesos técnicos seguidos por el sistema de IA, sino que basta con una descripción comprensible sobre los criterios seguidos para que el destinatario reciba un anuncio y no otro[121].

Algunas plataformas como Instagram ya ofrecen una opción para modificar dichos criterios. Esta medida es reflejo del considerando 68 DSA al aclarar que los prestadores «deben informar al destinatario de cualquier medio de que este disponga para modificar dichos

---

[119] Tato Plaza, A., Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia desleal*, La Ley Wolters Kluwer, 2010, pp. 130 ss.

[120] Considerando 69 DSA.

[121] Por ejemplo, cada anuncio de Instagram publicado en la sección feed, además de ser identificado como «anuncio», presenta una pestaña titulada «por qué ves este anuncio». Pongamos el ejemplo de un anuncio que recibimos sobre unos auriculares de la marca Marshall. Instagram nos informó de que la selección del anuncio obedecía a dos categorías de motivos. Por un lado, las opciones para anunciantes. La cuenta de @marshallheadphones había seleccionado que quería llegar a destinatarios mayores de 21 años, con ubicación principal en España. La sección detalla cómo sabe que el destinatario es mayor de 21 años (en este caso por facilitar la fecha de cumpleaños a la plataforma) y cómo ha determinado su ubicación principal (por la IP). Por otro lado, Instagram nos informó de que la selección se basaba en «nuestra actividad», indicando que previamente habíamos interactuado con publicaciones, historias, reels y páginas sobre música.

criterios»[122]. Sin embargo, es reseñable que ni la DSA ni la DMA establecen hasta la fecha la obligatoriedad de ofrecer alternativas menos personalizadas.

Aunque ambos Reglamentos tengan objetivos y ámbitos de aplicación distintos, su ámbito objetivo se solapa en muchos aspectos. Por ello, ciertas provisiones de la DMA pueden afectar a servicios regulados por la DSA, como exponíamos en apartados anteriores. Respecto a la posibilidad de modificar los criterios de selección, es destacable que los considerandos de la DMA señalen que los guardianes de acceso deberían ofrecer a los usuarios finales «una alternativa menos personalizada» que no condicione el acceso a la aceptación de ciertas combinaciones de datos entre diversos servicios y proveedores, generalmente con fines de publicidad personalizada[123]. Sin embargo, esta alternativa solo se incluyó como una recomendación y no como una obligación en el cuerpo normativo. La alternativa menos personalizada se ha venido reivindicando por muchos autores como una medida necesaria para asegurar la libertad de consentimiento de los sujetos de datos, especialmente para evitar modelos excesivamente intrusivos como el *pay-or-okay* de Meta[124].

En el caso de la publicidad personalizada, y desde un punto de vista puramente económico, es lógico que las empresas se vean reticentes a implantar un modelo dual ofreciendo una alternativa no basada en personalización. Un estudio de la CMA muestra que los medios ganan alrededor de un 70 por ciento menos cuando no pueden ven-

---

[122] A nuestro entender, la opción de modificar los parámetros publicitarios que ofrece Instagram es confusa y poco efectiva. Actualmente, ofrece la posibilidad de eliminar ciertos «temas», ordenados por interacciones recientes. Sin embargo, las etiquetas de estos temas son poco claras, al igual que los posibles filtros a aplicar. Pongamos el ejemplo de un destinatario que tiene un trastorno alimenticio y no desea visualizar contenidos relacionados con comida. Instagram no ofrece una vía para dejar de visualizar estos contenidos, tan solo ofrece una lista interminable de «temas» y categorías muy genéricas de filtros, como «cultura y sociedad». Esta imposibilidad de cambiar los parámetros de forma efectiva puede resultar en la explotación excesiva de vulnerabilidades del destinatario.

[123] Considerandos 36 y 37 DMA. En concreto, esta alternativa menos personalizada se recomienda cuando se lleve a cabo una de las prácticas contempladas en el art. 5 (2) de la DMA, las cuales están prohibidas salvo que el usuario final haya prestado su consentimiento conforme a los requisitos del RGPD. Las prácticas en cuestión son: *a)* tratar, con el fin de prestar servicios de publicidad en línea, los datos personales de los usuarios finales que utilicen servicios de terceros que hagan uso de servicios básicos de plataforma del guardián de acceso; *b)* combinar datos personales procedentes de los servicios básicos de plataforma pertinentes con datos personales procedentes de cualesquiera servicios básicos de plataforma adicionales o de cualquier otro servicio que proporcione el guardián de acceso o con datos personales procedentes de servicios de terceros; *c)* cruzar datos personales procedentes del servicio básico de plataforma pertinente con otros servicios que proporcione el guardián de acceso por separado, entre ellos otros servicios básicos de plataforma, y viceversa, y *d)* iniciar la sesión de usuarios finales en otros servicios del guardián de acceso para combinar datos personales.

[124] Sánchez Frías, I. «La prohibición de presentar publicidad…», *op. cit.*

der publicidad personalizada y compiten con otros que sí pueden[125]. En otras palabras, un menor nivel de personalización repercute en menor efectividad y, en consecuencia, en menos ingresos para los distintos operadores de la cadena de suministro. Desde el cumplimiento por diseño, un término medio de personalización podría ser la solución idónea para acomodar los intereses de los sujetos afectados. Así, el estudio pone de relieve que la pérdida total de la personalización publicitaria resultaría en anuncios irrelevantes y poco útiles para el consumidor, al mismo tiempo que resultaría en un modelo ineficiente para los anunciantes. Por ello, la solución óptima puede no ser introducir una opción no personalizada, sino una que resulte menos intrusiva o explotativa con respecto a posibles vulnerabilidades de los usuarios inferidas a raíz de su información personal[126].

El único ámbito en el que el legislador de la UE sí ha decidido incorporar la alternativa menos personalizada es en el de los sistemas de recomendación utilizados por VLOP y VLOSE. Así, el art. 38 de la DSA señala que los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño que utilicen sistemas de recomendación ofrecerán al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles tal como se define en el RGPD. Conforme al considerando 94, esta opción deberá ser directamente accesible desde la interfaz en línea en la que se presentan las recomendaciones. En teoría, la razón principal por la que esta obligación solo es aplicable a los sistemas de recomendación de las VLOP y VLOSE es por su especial papel como catalizadores de riesgos sistémicos, si bien estos riesgos también pueden concurrir en servicios distintos a los sistemas de recomendación.

Ahora bien, como señalábamos, el requisito de informar sobre los parámetros no es reseñable solo por su novedad, sino también por su complejidad. Para el propio prestador puede resultar complejo determinar con seguridad y claridad qué parámetros han sido considerados por el sistema de IA, sobre todo cuando el mismo es un sistema *deep learning* con poca trazabilidad. El cumplimiento de este requisito pasaría por optar por sistemas con un diseño transparente, así como someter el sistema de IA a continuas auditorías haciendo uso de mecanismos como los *sandboxes*. Si bien puede ser criticable que empresas con recursos más escasos tengan que hacer frente a estas complejas medidas de transparencia, no debemos olvidar que las obligaciones respecto al diseño y funcionamiento del sistema de IA se sitúan en el

[125] CMA, *Online platforms and digital advertising…, op. cit.*

[126] European Law Institute, *European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law, Response of the European Law Institute*, 2023, pp. 22-24.

prestador del servicio de intermediación publicitaria (generalmente, Alphabet, Meta y Amazon).

Lo deseable, por tanto, sería que estos distintos proveedores colaborasen para que el destinatario de la publicidad pueda ser informado con claridad sobre los principales parámetros utilizados. Los considerandos de la DSA señalan que en casos como este — en los que los riesgos se comparten entre plataformas en línea diferentes— los prestadores deben colaborar mediante la adopción de nuevos códigos de conducta, la suscripción de los ya existentes u otras medidas de autorregulación, especialmente en el caso de las obligaciones de transparencia relativas a la publicidad[127].

Por otro lado, puede suceder que el prestador de servicio de intermediación publicitaria se muestre reacio a colaborar con estos deberes de transparencia, alegando que el algoritmo publicitario empleado está protegido como información confidencial por secreto empresarial. Esta actitud puede estar fomentada no solo por una concurrencia real de información confidencial, sino también por el riesgo de que el algoritmo esté infiriendo datos sensibles o esté utilizando *proxies* con el objeto de evitar parámetros basados en datos sensibles y el prestador no tenga claro si dichas actividades constituyen una infracción de la prohibición, teniendo en cuenta las incertidumbres jurídicas que rodean al concepto de datos sensibles.

Sin embargo, como veníamos comentando, la norma no exige que el prestador publique un informe técnico detallado sobre el proceso seguido por el sistema de IA para seleccionar a los destinatarios. Al contrario, lo que exige es la publicación en la interfaz de información sobre los parámetros útil, sencilla y comprensible para el destinatario, con lo cual dificulta que el prestador justifique la puesta en peligro de secretos comerciales, ya que no se exige la desvelación de los procesos técnicos seguidos por el algoritmo publicitario.

Cuestión bien distinta es el posible requerimiento de acceso a datos por parte del coordinador de servicios digitales, si bien es una previsión limitada a las VLOP y a las VLOSE[128]. Como expondremos

---

[127] Considerandos (88) y (107) DSA. Una posible vía para que los principales prestadores de intermediación publicitaria colaboren mediante la autorregulación sería la incorporación a la European Advertising Standards Alliance (en adelante, EASA). EASA es el único organismo autorizado en materia de autorregulación publicitaria en Europa. Está compuesta por 28 organismos de autorregulación nacionales de 26 países europeos (entre los que se encuentra el organismo español Autocontrol) y 13 organizaciones de la industria publicitaria que abarcan publicidad impresa, exterior, TV, radio, marketing directo y publicidad digital e interactiva. Hasta la fecha, la única compañía digital global que se ha unido a EASA como miembro corporativo ha sido Google. Nota de prensa disponible en *https://www.autocontrol.es/2020/10/15/google-primera-compania-digital-global-que-se-une-a-easa-como-miembro-corporativo/.*

[128] Art. 40 DSA.

a continuación, dichos servicios quedan sujetos a una serie de normas de transparencia publicitaria adicionales.

VII. MEDIDAS ADICIONALES DE TRANSPARENCIA PUBLICITARIA APLICABLES A LAS VLOP

En caso de que alguno de los servicios de intermediación publicitaria que controlan el mercado actualmente (Alphabet Advertising, Meta Ads y Amazon Ads) fuese designado como VLOP, quedarían sujetos a una serie de obligaciones adicionales dirigidas a la gestión de riesgos sistémicos. Muchos de estos riesgos sistémicos reflejados en la propia norma guardan una estrecha relación con la prohibición de presentar publicidad basada en perfiles usando datos sensibles. La norma indica que en dichas evaluaciones de riesgos los prestadores deberán tomar en cuenta especialmente los sistemas de selección y presentación de anuncios, el diseño de sus sistemas algorítmicos y las prácticas relacionadas con los datos[129].

Uno de los riesgos sistémicos a evaluar por los prestadores de VLOP es la difusión de contenidos ilícitos a través de sus servicios. Teniendo en cuenta que la norma define como contenido ilícito todo aquel contenido que infrinja el derecho de la Unión o de uno de sus Estados miembros, la presentación de un anuncio basado en la elaboración de perfiles usando datos sensibles constituiría una difusión de contenido ilícito[130]. Otros ejemplos serían la inclusión de contenidos que no sean identificables como tales y puedan constituir publicidad encubierta.

También se han de evaluar como riesgos sistémicos los efectos negativos reales o previsibles para el ejercicio de derechos fundamentales. Un ejemplo sería la utilización de bases legales de tratamiento de datos personales que infrinjan el derecho a la protección de datos. En consecuencia, los prestadores de servicios de intermediación publicitaria que sean designados como VLOP deberían realizar evaluaciones de riesgo sobre las bases legales utilizadas para tratar datos personales con fines publicitarios, evaluación que se torna especialmente difícil si tenemos en cuenta las continuas disputas que rodean a la validez del consentimiento. Otro ejemplo sería la selección de destinatarios conforme a parámetros que infrinjan el derecho fundamental a la no discriminación que, como señalábamos en apartados anteriores, es el trasfondo de la prohibición de la DSA.

Los parámetros utilizados para seleccionar a los destinatarios de la publicidad también pueden explotar, por otro lado, ciertas vulnerabili-

---

[129] Art 34.2 DSA.

[130] Arts. 3.*h)* y 26.3 DSA.

dades y adicciones de las personas físicas[131]. Esta explotación podría constituir otro riesgo sistémico a evaluar, ya que la norma también señala como riesgo sistémico «las consecuencias negativas graves para el bienestar físico y mental de la persona»[132].

Las medidas que establece el art. 35 de la DSA para paliar estos riesgos son variadas. Una de ellas es la adaptación del diseño, las características y el funcionamiento de sus servicios, incluidas sus interfaces en línea. Un ejemplo de adaptación del diseño de la interfaz es la posibilidad que aporta Instagram de etiquetar ciertas publicaciones como «anuncios» para cumplir con las obligaciones de transparencia del art. 26 (1) DSA.

Otra medida de gran relevancia es la realización de pruebas y adaptación de sus sistemas algorítmicos. El diseño, entrenamiento y modificación del algoritmo publicitario es una medida esencial para asegurar el cumplimiento de la prohibición de presentar publicidad basada en perfiles utilizando datos sensibles.

Sin embargo, como hemos expuesto hasta el momento, la prohibición presenta numerosas lagunas, carencias e interrogantes. La mayor de estas lagunas se basa en sustentar la prohibición en la definición de datos sensibles del RGPD. Por un lado, hay ciertos datos —como los *proxies* y los datos inferidos— cuya calificación como sensibles no siempre es clara conforme al tenor del RGPD, el cual se muestra muy ajeno a los usos de datos personales, dependiendo excesivamente de la naturaleza extrínseca del dato personal en cuestión. Por otro lado, ciertos datos personales son excluidos de la lista cerrada de datos sensibles, pese a que en la práctica pueden ser utilizados con fines discriminatorios, produciendo efectos negativos en los destinatarios. Por estas razones, deviene necesario plantear si hay otras vías para evitar esos efectos perniciosos. La utilización del concepto de *vulnerabilidad* puede ser una buena alternativa para la construcción del sistema.

---

[131] Un ejemplo podría ser la personalización de anuncios en videojuegos *online* conforme a datos que revelen adicciones al juego del usuario, como exponíamos en otro lugar. Sánchez Frías, I. «El marketing algorítmico basado en datos reveladores de un trastorno por uso de videojuegos: un análisis desde el derecho de la competencia desleal», en Tato Plaza, A. *et al.* (coords.), *Nuevas tendencias en el Derecho de la Competencia…, op. cit.,* pp. 533-534.

[132] Art. 34 *d)* DSA.

SEGUNDA PARTE

LA EXPLOTACIÓN DE DATOS PERSONALES Y VULNERABILIDADES EN LAS PRÁCTICAS COMERCIALES BASADAS EN PERFILES. UN ANÁLISIS DESDE LA COMPETENCIA DESLEAL

CAPÍTULO IV

INFRACCIONES EN EL TRATAMIENTO, LA COMBINACIÓN Y LA EXPLOTACIÓN ILÍCITOS DE DATOS PERSONALES PARA LA OFERTA DE PUBLICIDAD BASADA EN PERFILES. UN REPROCHE DE DESLEALTAD POR VIOLACIÓN DE NORMAS

I. CONTEXTO ACTUAL DE LA VIOLACIÓN DE NORMAS

La normativa de competencia desleal española contiene un precepto con relativa presencia en el derecho comparado: la violación de normas, regulada por el art. 15 de la LCD[1]. Desde la introducción del precepto

[1] Señala Massaguer que el precepto no cuenta con precedentes en el derecho español ni en el comparado, sin que pueda ignorarse, no obstante, que la violación de normas constituye uno de los grupos de casos de infracción de la cláusula general de prohibición de la competencia desleal definido y caracterizado por la jurisprudencia y doctrina alemanas (*Rechtsbruch*). Massaguer Fuentes, J. «Artículo 15. Violación de normas», en Massaguer Fuentes, J. *Comentario a la Ley de Competencia Desleal*, *Civitas,* 1999, pp. 315-318.

En la actualidad, la Ley de Competencia Desleal alemana (en adelante, UWG) recoge también el supuesto de violación de normas como acto desleal en su sección 3a, el cual señala que «se considera desleal cuando una persona infringe una disposición legal que también tiene por objeto regular el comportamiento en el mercado en interés de los participantes en el mercado y la infracción de la ley puede perjudicar sensiblemente los intereses de los consumidores, otros participantes en el mercado y los competidores». Como es apreciable, la UWG contiene un supuesto único de violación de normas, a diferencia de la LCD española que, como analiza-

en la primera versión de la Ley en 1991 hasta la fecha, su aplicación no ha tenido una conexión clara con la infracción de la normativa relativa a los datos personales. Esta escasa relación empieza a sufrir un giro con el incremento del valor competitivo de los datos, de modo que ahora puede emplearse esta prohibición para actuar contra prácticas publicitarias basadas en datos personales que afecten a la equidad y disputabilidad de los mercados digitales, en infracción no solo de la normativa de protección de datos, sino también de la reguladora de la equidad en las relaciones interempresariales o de la disputabilidad de los mercados digitales.

En este sentido, algunos autores han señalado recientemente la relevancia de la violación de normas para hacer frente a prácticas comerciales desarrolladas a partir del tratamiento ilícito de datos personales[2]. Esta relevancia se ha materializado en la demanda presentada por parte de la Asociación de Medios de Información (en adelante, AMI) a Meta[3] por actos de competencia desleal sobre esa base[4].

A nivel de la UE, la complementariedad entre el RGPD y el ilícito de deslealtad por violación de normas ya ha sido advertida en el reciente caso *Lindenapotheke*[5]. En este caso se planteó al TJUE una cuestión prejudicial para que se pronunciase sobre la adecuación de la sección 3a de la UWG[6] a la normativa de la UE. Las consecuencias y fundamentos jurídicos de la sentencia son trasladables al caso español para interpretar el art. 15 de la LCD (regulador también de la denominada violación de normas). El TJUE confirma que el RGPD no se opone a una norma nacional que confiere a los competidores del presunto infractor del RGPD la legitimación activa para actuar contra este último mediante un recurso ante los tribunales civiles, por violaciones

---

remos, distingue entre la violación de normas concurrenciales y no concurrenciales. Para una comparación entre normativa española y alemana de competencia desleal, *vid.* Palau Ramírez, F. «La proyectada legislación alemana contra la competencia desleal y su valoración a partir de la legislación española», *Estudios sobre consumo*, núm. 67, 2003, pp. 27-30.

[2] Estevan de Quesada, C. «Data-protection related abuses by digital platforms: a Spanish enforcement alternative», en Ruiz Peris, J. I. y Estevan de Quesada, C. *New European Competition Trends…, op. cit.,* pp. 281-303. Colangelo, G. y Maggiolino, M. «Data Protection in Attention Markets: Protecting Privacy through Competition?», *Journal of European Competition Law & Practice*, vol. 8, núm. 6, 2017, pp. 363-369; Miranda Serrano, L. M. «Economía colaborativa y competencia desleal: ¿deslealtad por violación de normas a través de la prestación de servicios facilitados por plataformas digitales?», en *Revista de Estudios Europeos*, núm. 70, 2017, pp. 197-249.

[3] Sin resolución a fecha de envío del presente trabajo, en septiembre de 2025.

[4] Asociación de Medios de Información, «Los medios de información agrupados en AMI demandan a META por competencia desleal y reclaman más de 550 millones», *AMI*, 4 de diciembre de 2023, publicacion en línea.

[5] Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de octubre de 2024, *Lindenapotheke,* asunto C-21/23 (ECLI:EU:C:2024:846).

[6] Ley alemana contra la competencia desleal (Gesetz gegen den unlauteren Wettbewerb (cit. UWG).

a dicha norma y con base en la prohibición de prácticas comerciales desleales. En otras palabras, el Tribunal confirma que el RGPD no es incompatible con una norma nacional que legitime a los competidores o usuarios para demandar a un presunto infractor del RGPD por competencia desleal con base en dicha infracción.

A pesar de que esta aclaración del TJUE merece un juicio favorable, podría contestarse que no era estrictamente necesaria, puesto que el RGPD no tiene por objeto ni propósito regular las prácticas leales en el mercado. Dejando aparte posibles críticas, la sentencia presenta como cara positiva la reafirmación del carácter útil que puede rodear a una visión conjunta entre la normativa de protección de datos y de competencia desleal[7].

Así las cosas, como adelantábamos, la violación de normas ha comenzado a ganar protagonismo debido al valor económico de los datos personales y el modo en que las empresas pueden utilizar estos datos para llevar a cabo prácticas comerciales desleales. Pese a que el foco principal se sitúe en la ilicitud del tratamiento con fines publicitarios, tampoco debe desconocerse que este tratamiento no es la única conducta relacionada con los datos personales que puede resultar problemática desde el prisma de la competencia desleal. Otras actividades relacionadas con el tratamiento de datos personales (pero en cierto modo diferenciables de su procesamiento) han sido sometidas a una regulación específica en nuevas normas de derecho de la UE que funcionan como *lex specialis* respecto al RGPD. Nos referimos a la DMA y a la DSA, que fueron presentadas por la Comisión Europea de forma conjunta como el Paquete de Servicios Digitales. Ambos Reglamentos establecen prohibiciones relativas a la combinación de datos personales y a la presentación de publicidad basada en perfiles usando categorías especiales de datos personales.

Dada su redacción genérica, el art. 15 LCD se puede presentar como un instrumento viable para abordar aquellas prácticas que traten, combinen o exploten ilícitamente datos personales infringiendo las normas dedicadas a la protección de los derechos relacionados con estos datos y a disciplinar su uso. El reproche de deslealtad de estas conductas puede ser construido sobre las bases del art.15, sin ignorar, no obstante, que el precepto no funciona como una suerte de sanción añadida a aquella prevista por la norma infringida, sino que supone un ilícito distinto tendente a la prevención y represión de un éxito en el mercado que no se basa en la eficiencia de la oferta, sino en la actuación desde la ilegalidad[8].

---

[7] Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de octubre de 2024, *Lindenapotheke,* asunto C-21/23 (ECLI:EU:C:2024:846).

[8] Alfaro Águila-Real, J., «Competencia desleal por infracción de normas», *Revista de derecho mercantil*, núm. 202, 1991, pp. 667-669.

El ámbito general del art. 15 LCD se concentra en sus dos primeros apartados. En ellos se regula, respectivamente, la violación de normas generales (no concurrenciales) y, con alcance más específico, la infracción de las normas que tengan *por objeto la regulación de la actividad concurrencial*. Al ser los requisitos sensiblemente distintos según la norma sea concurrencial o no concurrencial, se torna necesario identificar qué carácter revisten las infracciones de las normas relacionadas con el tratamiento de datos personales y publicidad personalizada que pueden resultar problemáticos para el correcto funcionamiento del mercado, así como la naturaleza de las normas que los prohíben.

Si bien el análisis debe ser casuístico, distinguiremos tres supuestos generales de posible violación de normas: *a)* el tratamiento ilícito de datos personales por inválida aplicación de las bases legales previstas por el art. 6 del RGPD; *b)* la combinación ilícita de datos personales por infracción del art. 5.2 de la DMA; y *c)* la explotación ilícita de datos personales sensibles para presentar publicidad basada en perfiles, vulnerando el art. 26.3 de la DSA.

II. NOTAS PREVIAS EN TORNO A LA VIOLACIÓN DE NORMAS COMO PRÁCTICA DESLEAL

1. Cuestiones generales y finalidad del precepto

Desde su última modificación en 2022, la conducta desleal derivada de la infracción de normas del art. 15 LCD se descompone en cuatro ilícitos: dos de carácter general y dos de carácter específico. Estas conductas se vinculan entre sí tanto por el supuesto de hecho —a saber, una conducta de mercado infractora de normas jurídicas— como por la finalidad común perseguida —la represión del incumplimiento de obligaciones legales que generen o puedan generar situaciones de desigualdad entre los operadores económicos que concurren en el mercado—[9].

El primer apartado considera desleal prevalecerse en el mercado de una ventaja competitiva significativa adquirida mediante la infracción de leyes que no tengan por objeto la regulación de la actividad

[9] Por cuestiones de claridad, se reproduce a continuación la dicción del art. 15 LCD:

«1. Se considera desleal prevalerse en el mercado de una ventaja competitiva adquirida mediante la infracción de las leyes. La ventaja ha de ser significativa.

2. Tendrá también la consideración de desleal la simple infracción de normas jurídicas que tengan por objeto la regulación de la actividad concurrencial.

3. Igualmente, en el marco de lo dispuesto en el art. 2, se considera desleal la contratación de extranjeros sin autorización para trabajar obtenida de conformidad con lo previsto en la legislación sobre extranjería.

4. Igualmente, en el marco de lo dispuesto en el art. 2, se considera desleal el incumplimiento reiterado de las normas de lucha contra la morosidad en las operaciones comerciales».

concurrencial. El segundo apartado considera desleal *per se* la mera infracción de normas jurídicas que tengan por objeto la regulación de la actividad concurrencial. Por su parte, el apartado tercero considera desleal la contratación de extranjeros sin autorización para trabajar obtenida de conformidad con lo previsto en la legislación sobre extranjería, y el apartado cuarto considera desleal el incumplimiento reiterado de las normas de lucha contra la morosidad en las operaciones comerciales. Dado que los ilícitos de los apartados tercero y cuarto tienen un alcance específico que no se relaciona con el objeto de este estudio, nos centraremos a partir de ahora en la consideración del ilícito desleal por infracción de normas derivado de su configuración general en los apartados primero y segundo.

El objetivo común del precepto en todos sus apartados no es otro que garantizar la posición de igualdad ante la Ley de los operadores económicos en el juego competitivo (arts. 9 y 38 CE), prohibiendo las conductas que impliquen un aprovechamiento de las ventajas deslealmente obtenidas de no respetar la normativa imperativa frente a los competidores que sí cumplen con ella[10]. Esta ventaja puede derivar bien porque la infracción normativa permite mejorar la posición de ese agente concreto en el mercado, esto es, que produce una alteración de la *par conditio concurrentium* (art. 15.1 LCD); bien porque la violación de normas concurrenciales implica de por sí (salvo prueba en contrario) una distorsión o falseamiento de la igualdad en el mercado (art. 15.2)[11]. A este respecto sostenía Bercovitz que la libre competencia en el mercado parte de la base según la cual todos los competidores deben cumplir las obligaciones legales que les corresponden, razón por la cual se debe prevenir y reprimir la adquisición de una posición de ventaja frente a los competidores derivada del hecho de infringir normas jurídicas[12].

Como advertíamos, tanto la doctrina como la jurisprudencia del Tribunal Supremo señalan que la violación de normas del art. 15 no constituye una suerte de sanción añadida a la prevista por la norma vulnerada, sino que entraña un ilícito distinto al de la ilegalidad de la actuación al tiempo que una sanción distinta. Por ello, tampoco existe prejudicialidad ni vinculación del juez civil por la calificación que las autoridades competentes, en su caso, hayan podido hacer de los hechos[13]. Ahora bien, como sostienen ciertos autores —a cuya línea de opinión nos adscribimos— resulta

---

[10] Carbajo Cascón, F., «Violación de secretos, inducción y aprovechamiento de la infracción contractual e infracción de normas», en García-Cruces González, J. A. (coord), *Tratado de derecho de la competencia y de la publicidad*, vol. 2, Tirant lo Blanch, 2014, pp. 1528-1530.

[11] *Ibid.*

[12] Bercovitz-Rodríguez Cano, A. *Apuntes de derecho mercantil*, Aranzadi, p. 384.

[13] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* p.432; y Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* p. 668. Se hace

argumentable que el ilícito por deslealtad contribuye indirectamente al cumplimiento de dichas obligaciones, pues el reproche de deslealtad y la sanción correspondiente pueden sumarse a las sanciones previstas en la norma infringida[14].

2. Normas cuya vulneración puede activar la aplicación del precepto

Al analizar ciertas prácticas comerciales relacionadas con datos personales que se planteen como problemáticas, el primer paso será determinar (casuísticamente) si nos encontramos ante una violación normativa y si la norma infringida queda amparada por el supuesto de hecho del art. 15 LCD. Respecto a la norma infringida, existe acuerdo prácticamente unánime en la doctrina de que, por razones de coherencia sistemática, los dos primeros apartados del precepto deben interpretarse unitariamente, equiparando respectivamente los términos «leyes» y «normas jurídicas». En suma, la calificación de desleal no reside en un dato meramente formal, sino de naturaleza material, acogiendo normas de derecho positivo vinculantes que reúnan los caracteres de imperatividad, generalidad y coercibilidad, por lo que de su ámbito escapan aquellas normas de carácter dispositivo[15].

El ámbito material de las infracciones consideradas abarcaría tanto Reglamentos de la UE, leyes orgánicas y leyes ordinarias, decretos leyes, decretos legislativos, decretos, órdenes ministeriales, normativa análoga (legal y reglamentaria) de las Comunidades Autónomas, circulares del Banco de España, la CNMV y cualquier otra agencia independiente de control o regulación, las ordenanzas y reglamentos de entidades locales y también los estatutos generales y particulares de corporaciones profesionales, así como los convenios colectivos[16]. Como apuntan ciertos autores, una interpretación más restrictiva supondría obviar la posibilidad de que se obtenga una ventaja competitiva vulnerando normas de rango inferior a la ley formal, restringiendo

---

eco la jurisprudencia, entre otras, la STS de 13 de marzo de 2000 [RJ 2000, 1207], la STS de 29 de diciembre de 2006 [RJ 2007, 1714] y la STS de 17 de mayo de 2017.

[14] Sánchez Solé, S. «La violación de normas como acto de competencia desleal. [Comentario a la Sentencia de la Audiencia Provincial de Valencia (sección 6.ª) de 21 de marzo de 1994]», *RGD*, núm. 604-5, 1995, pp. 791ss; y Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.*; y Carbajo Cascón, F., «Violación de secretos, inducción…», *op. cit.*

[15] De forma contundente, Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.*; y en el mismo sentido se pronuncia Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-668; así como Sánchez Solé, S. «La violación de normas como…», *op. cit.,* pp. 791 ss.

[16] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.*

excesivamente la protección conferida por el art. 15 LCD[17]. El término *leyes* (en minúscula) se introdujo precisamente con el propósito de evitar que la deslealtad por infracción de esta clase de normas excluyera lo dispuesto en normas de rango inferior al legal, tales como decretos, órdenes ministeriales, ordenanzas municipales, etc.[18].

Pese a esta aceptación general, se excluyen de su ámbito objetivo ciertas disposiciones que por su relevancia para este trabajo deben tenerse en consideración. Alfaro y Massaguer defienden que se excluyen del art. 15 LCD aquellas normas jurídicas que reconozcan derechos subjetivos a los particulares, entre ellas las que reconozcan derechos de propiedad ordinaria y de propiedad industrial e intelectual y derechos de personalidad, como la propia imagen, ya que su violación afecta exclusivamente a la esfera individual del titular del derecho, que dispone de medios de tutela adecuados para su defensa[19]. Sostiene Massaguer que los terceros que pudiesen resultar mediatamente perjudicados a resultas de la actitud tolerante del titular del derecho hacia el infractor por la discriminación que ello les reporta deberán dirigirse al titular e instarle a ejercitar las acciones oportunas y, en su caso, valerse de los diversos mecanismos que proporciona el ordenamiento para sustituir al titular en el ejercicio de sus derechos[20].

Como analizaremos más adelante con ocasión de la violación de normas por infracción del RGPD, esta argumentación guarda matices cuando la infracción de una norma reguladora de derechos subjetivos de particulares se proyecta externamente sobre el correcto funcionamiento del mercado[21].

3. La distinción entre normas concurrenciales y no concurrenciales

Una vez determinada la infracción normativa y que la norma en cuestión es imperativa, general y coercible, el segundo paso será examinar si tiene o no como objeto regular la actividad concurrencial. De ello depende si la conducta se somete al apartado primero o al apartado segundo del art. 15 LCD, cuyos requisitos aplicables para el reproche de deslealtad son significativamente diferentes.

---

[17] Peñas Moyano, B., «La violación de normas concurrenciales y no concurrenciales como actos de competencia desleal», *Revista de Derecho de la Competencia y la Distribución*, núm. 3, 2008, pp. 209-232.

[18] Sánchez Solé, S. «La violación de normas como…», *op. cit.,* pp. 791 ss.

[19] Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730; y Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.*

[20] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-293.

[21] Entre otras, STS de 2 de marzo de 2009 [RJ 2009, 2789]

El apartado primero del art. 15 LCD se refiere a la infracción de normas no concurrenciales. Aunque la generalidad de la redacción del precepto exige un examen casuístico, la doctrina ha venido señalando ejemplos de normas que regulan la actividad concurrencial. A tal respecto señala Massaguer que se integra aquí la violación de cualquier norma susceptible de provocar costes, como son las normas fiscales y aduaneras, las normas laborales —incluidos los convenios colectivos, en tanto que regulan aspectos con repercusiones patrimoniales como son las normas sobre retribuciones, horario de trabajo, higiene y seguridad, prevención de riesgos laborales, seguridad social, etc.—, y, en general, de las normas que regulan mediata o inmediatamente la producción de bienes o prestación de servicios (como normas técnicas, normas sobre homologaciones, normas de protección o sobre procedimientos sanitarios, normas medioambientales…)[22]. Añade Palau que la violación de normas concurrenciales comprende también aquellas que regulan la autorización y condiciones para el acceso o el ejercicio de una profesión, las que regulan el acceso y las condiciones de competencia de un determinado sector, la normativa tuitiva de los intereses de los consumidores y la normativa que regula en general las condiciones de competencia, como la normativa sobre horarios comerciales y, más en particular, la normativa de ordenación del comercio y la Ley de Defensa de la Competencia[23].

Señala Carbajo que parece que el legislador de 1991 estaba pensando principalmente en la infracción de normas tributarias y de la seguridad social que dan lugar a lo que se conoce comúnmente como economía sumergida[24]. Cierta prueba de ello es que en la reforma de 2022 se introdujese un nuevo apartado en el art. 15 LCD (el cuarto), que califica también de desleal el incumplimiento reiterado de las normas de lucha contra la morosidad en las operaciones comerciales. Como advertíamos, el objeto de este capítulo es examinar la infracción de normas bien distintas, no relacionadas directamente con el ahorro de costes ni con la tributación o la seguridad social, sino aquellas que proscriben el tratamiento ilícito de datos personales, vetan su combinación en ciertos casos o prohíben usos concretos de los mismos.

La consecuencia principal de que la norma en cuestión sea una norma concurrencial es que su simple infracción constituirá *prima facie* un acto de competencia desleal. Por su propio impacto, el legislador presume que la mera infracción aporta automáticamente (al infractor

---

[22] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-300.

[23] Palau Ramírez, F. «Actos concretos de competencia desleal (I): por contrariar las exigencias de la buena fe; por explotación de la reputación ajena; por inducción a la infracción contractual; por violación de normas (arts. 4, 12, 14 y 15 LCD)», en Beneyto Pallás, K. (dir.), *Actos de competencia desleal y su tratamiento procesal: un estudio práctico de la Ley de competencia desleal* (LCD), Tirant lo Blanch, 2020, pp.70-72.

[24] Carbajo Cascón, F., «Violación de secretos, inducción…», *op. cit.,* pp. 1528-1530.

o al beneficiario) una ventaja competitiva significativa frente a los competidores que sí cumplen la norma, alterando el funcionamiento libre y no falseado del mercado y el aprovechamiento de la misma[25]. Ahora bien, esta presunción tiene carácter relativo (*iuris tantum*), pudiéndose rebatir si el demandado demuestra alguno de estos extremos: *a)* que la infracción no le ha reportado una ventaja competitiva, por ejemplo acreditando una situación de incumplimiento generalizado de la norma en los operadores del sector; *b)* que no se ha aprovechado de dicha ventaja competitiva; o *c)* que la ventaja no es significativa, es decir, que no guarda la suficiente relevancia para falsear la estructura competitiva del mercado.

Cuando la norma no tenga como objeto la regulación de la actividad concurrencial, se analizará por exclusión si el art. 15.1 de la LCD resulta aplicable. Si bien el precepto no hace referencia expresa a normas *no concurrenciales*, se entiende que este es el supuesto de hecho del precepto, por contraposición con respecto al art. 15.2. La distinción entre un apartado y otro es significativa ya que, mientras que en el caso de la infracción de normas concurrenciales opera la presunción *iuris tantum* anteriormente advertida, esta no opera en el caso de la infracción de normas no concurrenciales. Así las cosas, el examen casuístico del art. 15.1 pasará por los siguientes requisitos: *a)* la infracción de una norma no concurrencial; *b)* que a resultas de esa infracción se obtenga una ventaja competitiva para el infractor o para un tercero; *c)* que esa ventaja sea significativa; y *d)* que el infractor se prevalga en el mercado de tal ventaja significativa[26].

III. VIOLACIÓN DE NORMAS POR ILICITUD DE LA BASE LEGAL APLICADA AL TRATAMIENTO DE DATOS PERSONALES CON FINES DE PUBLICIDAD PERSONALIZADA. INFRACCIONES DEL RGPD

1. Identificación de la norma vulnerada. ¿Es el RGPD una norma amparada por el art. 15 LCD?

Entrando en el ámbito particular de la infracción de la normativa sobre protección de datos, la primera práctica que puede resultar problemática a efectos del art. 15 LCD es el tratamiento ilícito de datos personales. En estos casos, la principal norma infringida será el propio RGPD o la normativa de desarrollo que, en su caso, se haya aprobado en los distintos Estados miembros de la UE. Las causas por las que el tratamiento de datos puede ser ilícito bajo el articulado

[25] Emparanza Sobejano, A., «Artículo 15. Violación de normas», en Martínez Sanz, F. (dir.), *Comentario práctico a la Ley de competencia desleal,* Tecnos, Madrid, 2009, pp. 255-272.

[26] Bercovitz-Rodríguez Cano, A. *Apuntes de derecho mercantil…, op. cit.,* p. 384.

del RGPD no son escasas. Por cuestiones de coherencia con el objeto del presente trabajo, nos limitaremos a considerar exclusivamente la causa de ilicitud relativa a la invalidez de la base legal aplicada para el tratamiento[27]. Para determinar la aplicabilidad del art. 15 LCD en estos casos, es preciso establecer primero si la norma violada (en este caso, el RGPD) queda amparada por el supuesto de hecho del art. 15 LCD.

Formalmente, poca discusión cabe en señalar que el RGPD está amparado en el supuesto de hecho, ya que al tratarse de un Reglamento de la UE cumple con los caracteres formales de imperatividad, generalidad y coercibilidad[28]. Más discutible es si el RGPD es una norma amparada por el art. 15 LCD en un sentido material, para lo cual es necesario atender al propósito del precepto. La doctrina tiende a encuadrar la violación de normas como un ilícito contra el mercado, si bien reconoce que ciertos comportamientos pueden sufrir el reproche de deslealtad por vulnerar al mismo tiempo los intereses de los consumidores y los intereses de los competidores, además de las condiciones de competencia libre y no falseada en el mercado[29]. En este sentido, ciertos autores defienden que quedan excluidas aquellas normas que reconozcan derechos subjetivos a los particulares, entre ellos la propia imagen, ya que su violación afecta exclusivamente a la esfera individual del titular del derecho, que dispone de medios de tutela adecuados para su defensa[30].

Podría argumentarse que el RGPD es, por regla general, una norma en ciertos aspectos agnóstica en cuanto a los efectos del tratamiento, encontrándose casos en los que la acción ilícita afecta solo a la esfera privada (el derecho a la protección de datos) del individuo, sin necesidad de que se produzcan efectos perjudiciales para el mismo y mucho menos para el funcionamiento del mercado[31]. A título de ejemplo, el art. 5.1.*e)* del RGPD recoge el principio de «limitación del plazo de conservación», por el cual los datos personales deben ser eliminados o anonimizados tan pronto como no sean necesarios para el propósito

---

[27] Los motivos de esta acotación son principalmente dos. El primero es el reciente debate sobre la base legal aplicable a tratamientos de datos con fines de publicidad comportamental, en la que se inserta la publicidad basada en perfiles. El segundo es el papel que guarda la invalidez del consentimiento para la aplicabilidad de ciertas normas relativas a la combinación de datos personales (art. 5 (2) DMA).

[28] De forma contundente, Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318; y en el mismo sentido se pronuncian Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730; Sánchez Solé, S. «La violación de normas como…», *op. cit.,* pp. 791 ss.

[29] Por todos, Carbajo Cascón, F., «Violación de secretos, inducción…», *op. cit.,* pp. 1525-1622.

[30] Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730; y Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318.

[31] Para una crítica al agnosticismo del RGPD en cuanto a los usos aplicados a los datos personales, *vid.* Malgieri, G. *Vulnerability and Data…, op. cit.*

con el que fueron recogidos. Es posible que un responsable de tratamiento incumpla los plazos legales de conservación, pero este incumplimiento no perjudicará necesariamente al sujeto de datos, a los competidores o al libre funcionamiento del mercado. Lo relevante, a efectos del art. 15 LCD, es si el incumplimiento normativo ha sido un medio para adquirir una ventaja competitiva. El incumplimiento del plazo legal de conservación por sí solo no supone una ventaja competitiva: la ventaja puede derivar de los usos específicos aplicados a dichos datos y los efectos beneficiosos del incumplimiento. Estos extremos no son necesarios para que la autoridad de protección de datos sancione al responsable de tratamiento por una infracción del RGPD.

Así las cosas, el RGPD no requiere que se produzca un daño efectivo ni que el comportamiento ilícito rebase la esfera individual de los sujetos de datos afectados. Ahora bien, encontramos ciertas excepciones bajo la norma en las que la finalidad, el contexto o los efectos del tratamiento sí son tenidos en cuenta para declarar la ilicitud del tratamiento, pudiendo este examen guardar cierta relación con la esfera externa del sujeto de datos. Un ejemplo que veremos más adelante, con ocasión de la licitud del tratamiento de datos personales con fines publicitarios, es que la base legal de necesidad para el cumplimiento del contrato requiere una conexión entre los usos efectivamente aplicados a dichos datos y la necesidad de dichos usos para el cumplimiento del contrato[32]. Ejemplos como este justifican que el RGPD no deba ser descartado del supuesto de hecho del art. 15 LCD y que se aplique un examen caso por caso, teniendo en cuenta el precepto específico infringido.

En conclusión, pese a que el RGPD no regule de forma directa los usos aplicados a los datos personales, habrá situaciones en las que el incumplimiento de la norma facilite o pueda facilitar la adquisición de una ventaja competitiva, por lo que no resulta razonable excluir *prima facie* al RGPD del supuesto de hecho del art. 15 LCD. Cuestión bien distinta será justificar la deslealtad de la práctica, extremo que pasa primero por determinar si el RGPD es o no una norma concurrencial.

2. Calificación de la norma: El RGPD como norma no concurrencial

El problema fundamental de delimitación del ilícito de violación de normas consiste precisamente en determinar qué normas tienen por objeto regular la competencia en el mercado[33]. En este sentido,

[32] EDPB *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)*, y *EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR).*

[33] Carbajo Cascón, F., «Violación de secretos, inducción…», *op. cit.,* pp. 1525-1622.

la aproximación más práctica pasa por determinar si el RGPD cumple con los requisitos generales para catalogarse como una norma concurrencial (art. 15.2 LCD) y, en caso de que el resultado sea negativo, aplicar el art. 15.1 LCD.

En el plano formal, las normas vulneradas reguladoras de la competencia en el mercado pueden tener origen comunitario, estatal, autonómico o local, independientemente de su naturaleza pública o privada. En tal sentido, el RGPD podría ser una norma amparada por el art. 15.2 LCD desde una perspectiva estrictamente formal. Ahora bien, desde un plano material la respuesta no es tan directa. Entre las normas que tienen por objeto la regulación de la actividad concurrencial se suelen incluir las normas que diseñan la estructura del mercado (concediendo o justificando situaciones de monopolio u oligopolio, generales o territoriales), las normas sobre fijación directa o indirecta de precios en sectores concretos del mercado, las normas que ponen límites a posibles descuentos y las normas que regulan la actividad publicitaria[34]. Para calificar a estas normas como concurrenciales lo relevante no es que persigan la protección de la libre competencia, sino que se dirijan a regular el comportamiento concurrencial de los competidores, aunque no sea para garantizar el buen funcionamiento del mercado[35].

El objeto de la norma es, por tanto, el factor esencial para determinar si tiene o no carácter concurrencial. En lo que aquí nos atañe, el Tribunal Supremo aporta una regla clara: la norma en cuestión debe tener como objeto directo —y no reflejo o indirecto— la regulación de la actividad concurrencial, actividad a la que también se refiere como *comercial* o *mercantil*[36]. Siguiendo este requisito fundamental, el RGPD no sería una norma concurrencial, ya que su finalidad directa no es regular la actividad o comportamiento concurrencial de los competidores. El articulado del RGPD es claro al señalar que su objeto es la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de tales datos, protegiendo los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales[37].

---

[34] *Ibid.*

[35] Emparanza Sobejano, A., «Artículo 15. Violación de normas», *op. cit.,* pp. 255-272.

[36] STS 593/2000, 16 de junio de 2000 [RJ 2000, 5288]. En la sentencia, el TS también alude a la actividad concurrencial requerida como «comercial» y «mercantil», al señalar: «lo determinante es que tenga "por objeto" la regulación de la actividad comercial. Y este "objeto" debemos entenderlo como objeto directo y no indirecto o reflejo, pues de lo contrario no podría sostenerse la naturaleza privada del acto desleal que ha de considerarse como un "prius" de la ley para establecer el conocimiento de estos asuntos por la jurisdicción civil. Y la normativa que se invoca por el recurrente no tiene como objeto directo esta regulación mercantil» (Fundamento Jurídico tercero, con relación al art. 15 (2) LCD).

[37] Art. 1, apartados (1) y (2) RGPD.

Así las cosas, el objeto directo de la norma es claramente ajeno a la actividad concurrencial, por lo que el impacto de la norma sobre la actividad concurrencial solo podría apreciarse de forma refleja o indirecta. Esto nos lleva a concluir que el precepto a considerar debe ser el art. 15.1 LCD, relativo a la infracción de normas no concurrenciales. A esta misma conclusión llega de forma contundente Estevan de Quesada, añadiendo además que la aplicación del apartado segundo (violación de normas concurrenciales) no siempre lleva a eliminar el requisito de probar el prevalimiento de una ventaja significativa en el mercado como consecuencia de la infracción, puesto que este extremo puede ser discutido como defensa[38]. En otras palabras, si bien puede parecer que el examen de deslealtad bajo el apartado primero es más exigente al requerir en todo caso el prevalimiento de una ventaja significativa adquirida por infracción de leyes, la presunción de deslealtad del apartado segundo por violación de normas concurrenciales tiene carácter *iuris tantum*, admitiendo que el demandado alegue como defensa la no concurrencia de alguno de los requisitos exigidos.

3. Examen legal bajo el art. 15.1 LCD

3.1. *La infracción normativa. Ilicitud de la base legal aplicada para el tratamiento de datos personales conforme al RGPD*

Fijado el carácter no concurrencial del RGPD, el siguiente paso en aplicación del art. 15.1 LCD sería determinar si la práctica en cuestión constituye una infracción efectiva de la norma. Esta contravención no necesariamente debe ser consciente ni producirse con la intención específica de obtener una ventaja competitiva[39]. El presente apartado se acotará a tratamientos de datos personales con fines de publicidad personalizada en los que la base legal aplicada puede suponer o ha supuesto una infracción del RGPD.

Una cuestión que puede surgir es si es necesaria una resolución previa por parte de las autoridades competentes en materia de protección de datos. Existe consenso en que en la violación de normas no existe prejudicialidad ni vinculación del juez civil por la calificación que de los hechos hayan podido hacer, en su caso, las autoridades administrativas que pudieran conocerlos en el ámbito de sus competencias. Esta falta de vinculación agiliza la aplicación de la LCD a costa de problemas obvios[40]. Así las cosas, es necesario advertir que el juez civil apreciará si existe o no infracción legal a los solos efectos de constatar

[38] Estevan de Quesada, C. «Data-protection related abuses»…, *op. cit.,* pp. 281-299.

[39] Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730.

[40] *Ibid.*

el reproche de deslealtad y no de declarar la comisión de un ilícito a los efectos de la normativa considerada[41]. Desde una perspectiva práctica, entendemos que esta ausencia de vinculación se debe contemplar desde una justificación por celeridad. Cierta jurisprudencia considera que conviene extremar la prudencia en aquellos supuestos dudosos sobre los que todavía no exista resolución del órgano competente que declare la infracción legal[42].

En el ámbito de la aplicación de bases ilícitas para el tratamiento de datos personales, encontramos en España un precedente (sin resolver hasta la fecha) de violación de normas por incumplimiento del RGPD. En diciembre de 2023, la Asociación de Medios de Información (en adelante, AMI) presentó una demanda contra Meta en representación de 83 medios de información españoles por incumplimiento de la normativa europea de protección de datos[43]. Según el comunicado de prensa de AMI, la utilización sistemática y masiva de datos personales obtenidos ilícitamente de los usuarios de las plataformas de Meta habría permitido a la empresa ofrecer en el mercado la venta de espacios publicitarios a partir de una ventaja competitiva ilegítimamente obtenida[44].

Si bien no existe prejudicialidad ni vinculación del juez civil, la existencia de una resolución vinculante del CEPD respecto a la ilegalidad de bases legales aplicadas por Meta para recabar datos con fines publicitarios puede ser relevante para reducir el margen de dudas en cuanto a una infracción normativa por Meta. En este sentido, el CEPD emitió en diciembre de 2022 dos decisiones vinculantes en las que declaraba ilícita la base legal de necesidad para el cumplimiento del contrato (art. 6.1.*b)* RGPD) en Instagram y Facebook para tratar datos personales con fines de publicidad comportamental, infringiendo adicionalmente los principios de licitud del tratamiento y transparencia [art. 5.1.*a)* RGPD][45][46]. La decisión vinculante provocó que la

---

[41] SAP Albacete de 23 de marzo de 1993.

[42] *Ibid.*

[43] Asociación de Medios de Información, «Los medios de información agrupados…», *op. cit.*

[44] *Ibid.*

[45] EDPB *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)*, y *EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR).*

[46] Haciendo un breve sumario de los puntos clave de la decisión, el CEPD recuerda que, para la evaluación de la necesidad con arreglo a esta base jurídica, es importante determinar la razón exacta del contrato (es decir, su contenido y su objetivo fundamental). Además, se requiere que el tratamiento sea objetivamente necesario para la prestación de ese servicio contractual al interesado. El análisis por parte del CEPD de la perspectiva del usuario en el momento de la celebración del contrato reviste especial importancia, ya que la prueba de necesidad depende no solo de la perspectiva del responsable del tratamiento (en este caso, Meta), sino también

Autoridad Irlandesa de Protección de Datos sancionase a Meta con una multa de 390 millones de euros (210 millones de euros en relación con Facebook y 180 millones de euros en relación con Instagram)[47].

Si bien el CEPD reconoció en su decisión vinculante que Meta no está obligada a establecer el consentimiento como base legal, ciertos autores señalan que el margen de bases legales a aplicar tras esta resolución es parco[48]. La mencionada sanción provocó una cadena de bases legales cuya licitud continúa sin ser clara.

Siguiendo un desarrollo cronológico, en marzo de 2023, Meta anunció la aplicación de la base legal de interés legítimo para continuar tratando datos personales con fines de publicidad comportamental. Esta iniciativa fue cancelada en julio del mismo año a raíz del cono-

---

de las expectativas razonables del usuario, ya que el concepto de «necesidad» tiene su propio significado autónomo en el derecho de la Unión.

El CEPD tiene en cuenta algunos hechos para la prueba de necesidad. En primer lugar, el hecho de que las Condiciones de Uso no prevén ninguna obligación contractual por parte de Meta IE para ofrecer publicidad personalizada a los usuarios de Instagram, así como tampoco ninguna penalización contractual en caso de que Meta IE no preste este servicio. En segundo lugar, el CEPD considera que el estado de necesidad no se deriva del modelo de negocio de Meta IE de ofrecer servicios a cambio de emitir publicidad comportamental. En tercer lugar, el CEPD tiene en cuenta si existen alternativas realistas y menos intrusivas; de ser así el tratamiento no es «necesario». El CEPD afirma que existen alternativas realistas y menos intrusivas que la publicidad comportamental, como la publicidad contextual basada en la geografía, el idioma y el contenido, que no implican medidas intrusivas como la elaboración de perfiles y el seguimiento de los usuarios (*profiling and tracking*). En cuarto lugar, el CEPD considera que un usuario razonable no puede esperar que sus datos personales se traten con fines de publicidad comportamental por el mero hecho de que Meta IE se refiera brevemente a este tratamiento en sus condiciones de uso de Instagram. El CEPD argumenta que las expectativas del interesado medio deben tenerse en cuenta a la luz no solo de las condiciones del servicio, sino también de la forma en que este servicio se promociona a los usuarios. En este caso, la misión del servicio de Instagram, tal y como se expresa en sus Condiciones de Uso, se formula de manera vaga y amplia: «Acercarte a las personas y las cosas que amas». Según el CEPD, la falta de necesidad de la publicidad como parte del servicio prestado se confirma por la descripción del servicio de Instagram que hace IE SA en su proyecto de Decisión: «Instagram es un servicio global de red social en línea que permite a los usuarios registrados comunicarse con otros usuarios registrados a través de mensajes, audio, videollamadas y chats de vídeo, y mediante el envío de imágenes y archivos de vídeo».

Por estas razones, la Decisión Vinculante concluye que la publicidad comportamental realizada por Meta en el contexto del servicio de Instagram no es objetivamente necesaria para la ejecución del contrato de Meta IE y no es un elemento esencial o central del mismo.

[47] Irish Data Protection Commision, Decision of December 31, 2022, DPC Inquiry Reference: IN-18-5-5; and Decision of December 31, 2022, DPC Inquiry Reference: IN-18-5-7.

[48] Nosotros mismos y Castillo Parrilla, J.A. «"Pay or ok". Pagar con datos personales tras la Directiva 2019/770: una visión comparada entre España y Portugal», *Revista Electrónica de Direito*, 2024, pp. 102-144. Siguiendo el razonamiento del CEPD, entendemos que una posible vía para poder continuar aplicando la base legal de necesidad para la ejecución del contrato hubiera sido optar por una publicidad menos intrusiva, como puede ser la publicidad contextual. Así, en apartados anteriores veníamos señalando la deseabilidad de fomentar la introducción de alternativas menos personalizadas en publicidad, si bien parece que esta opción fue rechazada por Meta en vista de las posteriores bases legales que la empresa decidió aplicar.

cido caso *Meta Platforms Inc. v. Bundeskartellamt,* en el que el TJUE declaró la falta de adecuación de la base legal de interés legítimo para la personalización de publicidad[49]. El Tribunal señaló expresamente que «pese a la gratuidad de los servicios de una red social en línea como Facebook, el usuario de esta no debería esperar razonablemente que, sin su consentimiento, el operador de esa red social trate los datos personales de ese usuario con fines de personalización de la publicidad. En estas circunstancias, debe considerarse que los intereses y los derechos fundamentales de tal usuario prevalecen sobre el interés de dicho operador en tal personalización de la publicidad, mediante la que él financia su actividad, de modo que el tratamiento efectuado por este para tales fines no puede estar comprendido en el ámbito de aplicación del art. 6, apartado 1, párrafo primero, letra *f)*, del RGPD» (es decir, el interés legítimo).

La consecuencia de este pronunciamiento fue que Meta implementase el controvertido modelo conocido como *pay-or-okay* o *pay-or-consent.* Paradójicamente, el modelo se formuló originariamente como una vía para proteger a los periódicos digitales frente a *Big Techs* como Meta, contando inicialmente con la aprobación condicionada de varias autoridades de protección de datos como la alemana[50], la francesa[51] y la española[52]. Esta ironía se acentúa si tenemos en cuenta que más de 80 periódicos españoles han demandado a Meta por competencia desleal sobre la base del tratamiento ilícito de datos personales con fines publicitarios.

Meta escudó la legalidad de su modelo precisamente en la mencionada STJUE *Meta Platforms Inc. v. Bundeskartellamt,* en la cual el Tribunal declaró que los usuarios de redes sociales como Facebook deben disponer de la libertad de negarse individualmente a prestar su consentimiento a fines de tratamiento no estrictamente necesarios, sin verse por ello obligados a renunciar íntegramente a la utilización del servicio de red social, lo que implica que se ofrezca, en su caso,

---

[49] Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023, asunto C-252/21, *Meta Platforms y Bundeskartellamt* (ECLI:EU:C:2023:537), párrafo 117.

[50] *Vid.* Resolución de la Conferencia de Autoridades Independientes de Control de Protección de Datos Federales y Estatales de 22 de marzo de 2023, «Evaluación de los modelos de suscripción pura en el sitio web».

[51] La autoridad francesa de protección de datos (CNIL) emitió unas directrices en 2020 en las que señalaba que el análisis de su legalidad debe ser caso por caso. *Vid.* CNIL, «Cookie walls: la CNIL publie des premiers critères d'évaluation», versión actualizada de 2022.

[52] La autoridad española de protección de datos AEPD tampoco ha declarado la ilegalidad absoluta de modelos de *cookie walls* como el *pay-or-okay,* al señalar que «(p)odrán existir determinados supuestos en los que la no aceptación de la utilización de cookies impida el acceso al sitio web o la utilización total o parcial del servicio, siempre que se informe adecuadamente al respecto al usuario y se ofrezca una alternativa, no necesariamente gratuita, de acceso al servicio sin necesidad de aceptar el uso de cookies». *Vid.* AEDP, *Guía sobre el uso de cookies*, 2024.

«a cambio de una remuneración adecuada, una alternativa equivalente no acompañada de tales operaciones de tratamiento de datos».

El primer pronunciamiento sobre la legalidad del *pay-or-okay* por parte de una institución de la Unión fue una opinión del CEPD, en la que el Comité se mostró contundentemente en contra de la legalidad del modelo, afirmando que «en la mayoría de los casos, no será posible que las grandes plataformas en línea cumplan con los requisitos para un consentimiento válido cuando confrontan al usuario solo con una opción binaria entre consentir el tratamiento de datos personales para publicidad comportamental o pagar una tasa»[53].

En abril de 2025, la Comisión Europea finalmente aplicó una sanción de 200 millones de euros a Meta por la ilegalidad de su modelo *pay-or-okay*. Ahora bien, de esta decisión de la Comisión hay que destacar dos extremos. El primero, que la sanción se enmarca en una infracción del art. 5 de la DMA, y no del RGPD aisladamente, como tendremos ocasión de analizar. El segundo, que la decisión opera sobre el primer modelo de *pay-or-okay* instaurado por Meta, y no sobre el segundo implementado a partir de noviembre de 2024, sobre el cual todavía no hay pronunciamiento. Así las cosas, la sanción opera sobre el modelo *pay-or-okay* en un marco temporal concreto, que abarca desde marzo de 2024 (cuando las obligaciones del art. 5 DMA entraron en vigor) hasta noviembre de 2024 (cuando se instauró el segundo modelo *pay-or-okay*), y resulta de la aplicación del art. 5 de la DMA, si bien en relación con un tratamiento ilícito de datos conforme al RGPD.

Concluyendo, si bien el juez civil no está vinculado por decisiones previas de la Comisión Europea, las mismas podrían (y entendemos que deberían) ser tenidas en cuenta para declarar la infracción del RGPD a efectos de aplicar el art. 15.1 LCD en lo respectivo a aquellos períodos en los que el prestador en cuestión haya aplicado bases ilícitas de tratamiento. Siguiendo el ejemplo de la demanda a Meta por los periódicos españoles, aun en el caso de que el juez civil aprecie una infracción normativa, quedaría determinar el resto de los requisitos del art. 15.1 LCD, esto es, prevalerse en el mercado de una ventaja competitiva significativa adquirida mediante la infracción.

---

[53] EDPB, Opinion 08/2024 on Valid Consent In The Context Of Consent Or Pay Models Implemented By Large Online Platforms, 2024, par. 179. Como su propia denominación indica, la «opinión» no tiene carácter vinculante, si bien puede servir de guía para las autoridades nacionales de protección de datos. European Commission, «Commission finds Apple and Meta in breach of the Digital Markets Act», 23 de abril de 2025.

3.2. *Adquisición de una ventaja competitiva significativa como resultado del tratamiento ilícito de datos personales*

A. La obtención de una ventaja competitiva

Comenzando por el primer factor, entiende la doctrina que la ventaja competitiva se produce cuando la violación de normas permite al infractor mejorar su posición respecto a los competidores y conseguir de este modo desarrollar su actividad en términos más atractivos para sus clientes, mejora que no hubiera podido lograr sin la infracción de la norma en cuestión[54]. En el caso de los datos personales, numerosos estudios jurídicos y económicos destacan el valor comercial de los datos en los mercados digitales[55]. Este fenómeno ha dado lugar a tópicos como «los datos son el nuevo petróleo» o a la consideración de la denominada *data-advantage* (ventaja de los datos)[56].

Como reconoce Estevan de Quesada, las perspectivas sobre el valor competitivo de los datos pueden ser diversas. Destaca el hecho de que los datos son ubicuos, baratos, fáciles de recopilar, no exclusivos y no rivales, señalando que, al ser un bien público y accesible a todos, nunca podrían constituir una ventaja competitiva o una barrera para entrar en el mercado. Otros estudios han analizado la *ventaja de los datos* resultante de la acumulación y procesamiento de grandes cantidades y variedades de datos por parte de las plataformas digitales, algo que ocurre especialmente bajo ciertas circunstancias[57]. Entre estas circunstancias se destacan aquellas en las que: *a)* los datos son excluyentes, *b)* contribuyen a efectos de aprendizaje que pueden ser utilizados para mejorar el producto o servicio, *c)* se utilizan para orquestar interacciones en una red, *d)* existen economías de escala y alcance junto con activos complementarios para utilizarlos (como algoritmos) y *e)* existe una competencia dinámica débil.

En lo que aquí nos atañe, lo necesario no es probar el valor comercial de los datos, sino que los datos personales obtenidos ilícitamente hayan derivado en una ventaja competitiva significativa de la cual el infractor o el beneficiario se prevalga. Este extremo nos lleva

---

[54] Emparanza Sobejano, A., «Artículo 15. Violación de normas», *op. cit.,* pp. 255-272.

[55] Cabral, L. *et al.*, *The EU Digital Markets Act…*, *op. cit.*

[56] EU Commissioner Kroes speech, disponible en: *http://europa.eu/rapid/press-releaseSPEECH-1 2-149_en.htm.*

[57] Autorité de La Concurrence y Bundeskartellamt. *Competition Law and Data*, 2016; Furman, J. *et al.*, *Unlocking digital competition. Report of the Digital Competition Expert Panel (Furman Report),* 2019, pp. 32-35; Comisión Europea (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions). «A European Strategy for Data», COM(2020) 66 final, p. 9.

a plantear el segundo requisito: la causalidad entre la infracción y la ventaja competitiva.

B. La relación de causalidad entre la infracción y la ventaja competitiva

La violación de normas no concurrenciales exige un segundo requisito: probar la relación de causalidad entre la infracción y la ventaja competitiva o, en otras palabras, que la ventaja competitiva no hubiese podido adquirirse de no ser por la infracción normativa. Aunque el RGPD tiene como función directa la protección de los datos personales de las personas físicas, la infracción de esta protección resulta en el acceso a datos personales que permiten optimizar las tasas de efectividad de la publicidad digital personalizada, ya sea aumentando el número de clics sobre el anuncio, las ventas sobre el producto o servicio, las visualizaciones, los «me gusta» o cualquier otro tipo de interacción entre el sujeto de datos y la publicidad personalizada. Esta alta efectividad puede dar lugar a que la plataforma ofrezca un servicio de intermediación publicitaria mucho más atractivo para los anunciantes con respecto a otros competidores, atractivo que es considerado por la doctrina para analizar si se produce el supuesto de hecho del art. 15.1 LCD.

La relación de causalidad entre el uso de bases ilícitas y la ventaja competitiva puede llegar a apreciarse en el hecho de que Alphabet sea uno de los tres principales prestadores de servicios de intermediación publicitaria *online* junto con Meta y Amazon. Es destacable que solo los servicios publicitarios de estos han sido designados como servicios básicos de plataforma con base en la DMA, si bien previamente a esta designación conocidos informes apuntaban ya a Meta como uno de los principales prestadores del oligopolio imperante en la intermediación publicitaria[58].

Por otra parte, no debemos pasar por alto que en el caso de Alphabet, Meta y Amazon, sus servicios de publicidad se integran también en otros servicios del mismo prestador (como redes sociales o *marketplaces*). De ello resulta que el tratamiento ilícito pueda suponer una ventaja competitiva en dos ámbitos: en el publicitario, haciendo que su servicio de intermediación sea más deseable para los anunciantes, y en el de los demás servicios principales prestados, ya que el contenido de muchos de ellos también es personalizado conforme al perfil de cada usuario[59].

---

[58] Cabral, L. *et al.*, *The EU Digital Markets Act…*, *op. cit.*

[59] Esta variedad de servicios concentrados en una misma empresa ha dado lugar a prohibiciones en la DMA que analizaremos más adelante.

Concluyendo, si bien el examen debe realizarse casuísticamente, en aquellos casos en los que la cantidad y la variedad de datos obtenidos ilícitamente hayan contribuido a mejorar la posición de mercado y la eficiencia del servicio de publicidad y/o del servicio principal cabría afirmar la relación de causalidad entre la infracción y la ventaja competitiva.

C. La ventaja competitiva «significativa» para el infractor o para un tercero. ¿Concurre la excepción de incumplimiento generalizado en el caso del *pay-or-okay*?

El art. 15.1 LCD exige no solo la adquisición de una ventaja competitiva, sino que dicha ventaja sea *significativa*. Se considera significativa aquella ventaja de una magnitud apreciable, y debe tener un alcance de nivel tal que pueda provocar o de hecho provoque una desviación de clientela o que obligue a los competidores a reducir sus márgenes o a realizar cualquier clase de esfuerzo innovador o de mejora (que, en tales circunstancias, no permitirá alcanzar la recompensa que merece) para estar en condiciones de neutralizar la ventaja debida a la infracción de la norma[60].

En lo que aquí nos atañe, las actividades relacionadas con los datos tienen, en principio, un impacto significativo en las posiciones de mercado debido a las características de los mercados digitales, si bien la evaluación del carácter significativo de la ventaja competitiva dependerá de las características específicas del mercado de referencia y requerirá un análisis caso por caso, tanto en lo que se refiere a la importancia de los datos en ese mercado, como a la pertinencia de la ventaja obtenida en comparación con la situación de los competidores[61].

Señalan algunos autores que un factor a considerar en este examen casuístico debe ser la proporción de mejora de la posición competitiva atribuible a la infracción. Esta proporción de mejora podría calcularse comparando las posiciones de mercado del infractor antes y después de la infracción normativa, con el fin de evaluar si la posición en el mercado ha mejorado y en qué medida[62]. En este análisis se tendría que examinar si otros factores competitivos siguen siendo los mismos, ya que la mejora de la posición en el mercado puede deberse a otras razones diferentes de las actividades relacionadas con los datos, como un avance tecnológico o una innovación desarrollada por el infractor[63]. Siguiendo el ejemplo de Meta, es cierto que pueden concurrir avances

---

[60] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318.

[61] Estevan de Quesada, C. «Data-protection related abuses…», *op. cit.,* pp. 281-303.

[62] Por todos, Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318.

[63] Estevan de Quesada, C. «Data-protection related abuses…», *op. cit.,* pp. 281-303.

tecnológicos en su algoritmo o sistema de IA de intermediación publicitaria que hayan facilitado la optimización de la publicidad personalizada en los últimos años.

Sin embargo, no debemos olvidar que cualquier mejora en los sistemas algorítmicos o sistemas de IA depende de la cantidad, variedad y calidad de los *inputs*. En el caso de los sistemas de IA utilizados con fines publicitarios, los datos personales de los usuarios son imprescindibles para que el sistema resulte más efectivo, por lo que el tratamiento ilícito de los mismos está directamente relacionado con los avances tecnológicos del infractor y con la posible mejora de su posición de mercado. En otras palabras, no concurren razones ajenas al uso de datos que justifiquen la posible mejora de la posición de Meta en el mercado digital de la intermediación publicitaria. El examen pasaría entonces por analizar su posición antes y después de aplicar bases legales de tratamiento que sean ilícitas conforme al RGPD.

Otros autores señalan como factor determinante del carácter significativo de la ventaja la existencia de una violación jurídica sistemática, ya que es raro que infracciones aisladas y puntuales puedan aportar ventajas significativas[64]. Continuando con el ejemplo de Meta, el hecho de que la misma haya aplicado sistemáticamente bases legales ilícitas (por orden cronológico: necesidad para la ejecución del contrato, interés legítimo y, discutiblemente, consentimiento sobre una opción *pay-or-okay*) podría ser otro indicador de que la ventaja competitiva es significativa.

Aun asumiendo que se cumplen todos los requisitos del art. 15.2 LCD, siguiendo el ejemplo del modelo *pay-or-okay*, cabría plantear una cuestión que no debemos pasar por alto. ¿Afecta la aplicación generalizada de una base legal ilícita al reproche de deslealtad? O, más concretamente, ¿el hecho de que el modelo *pay-or-okay* se aplique por una generalidad de competidores influye en la ventaja competitiva significativa adquirida por Meta? A título de ejemplo, en la sentencia de 17 de mayo de 2017, el Tribunal Supremo entendió que no hay deslealtad ante un incumplimiento generalizado de la normativa sobre juego. Si bien esta resolución ya ha sido criticada por algún autor[65], debe destacarse que la sentencia en cuestión no solo se basó en el incumplimiento generalizado sino también en el carácter obsoleto

[64] Emparanza Sobejano, A., «Artículo 15. Violación de normas…», *op. cit.,* pp. 255-272; y Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730.

[65] A juicio de Palau, esta aproximación haría perder el carácter neutral de la LCD, que impide hacer política de la competencia en su aplicación, y se obliga a asumir las reglas de competencia, dictadas en aras de proteger intereses públicos y con respeto a la Constitución económica. No obstante, el autor también destaca que en la referida sentencia el TS se fundamenta también en el carácter obsoleto de las normas aplicables al caso. Palau Ramírez, F. «Actos concretos de competencia desleal (I)…», *op. cit.,* p. 67.

de las normas infringidas. Con más matices señalan algunos autores que el reproche de deslealtad debe decaer «en la medida en la que los operadores del particular mercado incumplan de modo generalizado y en igual forma la norma en cuestión»[66].

La pregunta que planteábamos es, en cierto modo, capciosa. El hecho de que una generalidad de competidores aplique el modelo *pay-or-okay* no es sinónimo de que concurra un *incumplimiento generalizado*, ya que el examen de ilicitud del modelo *pay-or-okay* debe ser casuístico, lo que dificulta que nos encontremos ante dicha excepción por dos categorías principales de razones.

La primera se refiere a las posibles divergencias en cuanto a los infractores. En la conocida sentencia *Bundeskartellamt*[67], el TJUE declaró que la posición de dominio no es determinante pero sí relevante a la hora de dilucidar si el consentimiento del sujeto de datos ha sido prestado libremente. En este mismo hilo, entendemos que la aplicación del *pay-or-okay* por los periódicos digitales no debe ser un obstáculo para declarar una violación de norma por parte de Meta, ya que la posición de mercado de dichos prestadores es sensiblemente diferente. En el mismo sentido, el CEPD ha señalado que el examen de licitud del consentimiento debe realizarse teniendo en cuenta el tamaño del responsable de tratamiento, si bien nos encontramos solo parcialmente de acuerdo con la justificación jurídica aportada por el Comité[68].

La segunda categoría de razones radica en la necesidad de realizar un examen de las características específicas de cada modelo de consentimiento. Pese a que el denominador común de todos los modelos *pay-or-okay* es una opción binaria, las condiciones y el contexto pueden

---

[66] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318.

[67] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 4 de julio de 2023, asunto C-252/21, *Meta Platforms y Bundeskartellamt* (ECLI:EU:C:2023:537).

[68] EDPB, Opinion 08/2024 on Valid Consent In The Context Of Consent Or Pay Models Implemented By Large Online Platforms, 2024. Si bien no es objeto del presente trabajo realizar una crítica exhaustiva de la opinión emitida por el CEPD a propósito del *pay-or-okay*, vemos necesario destacar la escasa rigurosidad o claridad jurídica de la opinión al introducir un nuevo término, al que denomina «grandes plataformas *online*» (*large online platforms*) y cuya definición se circunscribe inicialmente a la opinión emitida. El CEPD señala que el concepto abarca «entre otros» a las plataformas *online* en el sentido de la DSA y a los guardianes de acceso en el sentido de la DMA, subrayando que el término no se limita solo a los anteriores prestadores, debiendo someterse a un examen caso por caso. Más que una definición, el CEPD aporta un concepto jurídico indeterminado que puede desencadenar una gran inseguridad jurídica para los responsables de tratamiento. A nuestro entender, el CEPD podría haberse limitado a referirse a los VLOPs en el sentido de la DSA y a los guardianes de acceso en el sentido de la DMA como ejemplos en los que el desequilibrio de poder es más evidente y la libertad de consentimiento puede ponerse en entredicho. Estos dos conceptos (VLOPs y guardianes de acceso) son fruto de un proceso legislativo largo con requisitos normativos que, aunque imperfectos, presentan una mayor claridad para los responsables de tratamiento. Introducir un tercer término en el que apenas se esbozan unas características mínimas puede tener como efecto incrementar hiperregulación y la inseguridad jurídica a efectos de cumplimiento normativo.

ser diferentes. Como señala el CEPD, el análisis de licitud del consentimiento en estos modelos debe tener en consideración diversos factores, como el nivel de detrimento del sujeto de datos en el caso de rechazar el tratamiento con fines de publicidad comportamental, el desequilibrio de poder, la existencia de una alternativa equivalente, el carácter apropiado de la suma a pagar y la granularidad del consentimiento[69]. Igualmente, la decisión de la Comisión Europea en la que sanciona a Meta por la ilegalidad de su primer modelo *pay-or-okay* afecta, exclusivamente, a la empresa infractora. No podía ser de otra manera, vista la propia naturaleza del acto jurídico (una decisión sancionadora), la cual difiere notablemente de los actos del poder legislativo competente para establecer prohibiciones absolutas en la materia.

La necesidad de realizar un examen caso por caso nos lleva a apuntar la posibilidad de que el modelo implementado por Meta en sus redes sociales sea declarado ilícito conforme al RGPD, pero dicha ilicitud no se declare en otros servicios, como algunos periódicos *online*. Entendemos que una aplicación lícita del *pay-or-okay* por los periódicos digitales u otros competidores no es excluyente de una violación de la norma por parte de Meta, ya que la posición de mercado de dichos prestadores es sensiblemente diferente y las condiciones de cada modelo pueden diferir.

En conclusión, la necesidad de seguir un complejo examen casuístico sobre bases legales de tratamiento, como el *pay-or-okay,* nos lleva a concluir la improbabilidad de que se pruebe la excepción de un *incumplimiento generalizado* del RGPD. Habría que atender a los mencionados indicadores de adquisición de una ventaja significativa que revelen, entre otros factores, la desviación de clientela (en este caso, los anunciantes) hacia el servicio de intermediación publicitaria del infractor y la necesidad de los competidores de reducir sus márgenes o de realizar cualquier clase de esfuerzo innovador o de mejora (que, en tales circunstancias, no permitirá alcanzar la recompensa que merece) para estar en condiciones de neutralizar la ventaja debida a la infracción de la normativa de protección de datos.

D. El prevalimiento de la ventaja significativa

El art. 15.2 de la LCD no exige solo la adquisición de una ventaja competitiva significativa como consecuencia de la infracción, sino, además, el prevalimiento de esta. Entiende la doctrina que este prevalimiento se produce cuando el infractor se beneficie en costes financieros, en tiempo o de otra forma que se traslade al proceso de producción

[69] EDPB, *Opinion 08/2024 on Valid Consent In The Context Of Consent Or Pay Models Implemented By Large Online Platforms*, 2024.

y distribución[70]. El factor esencial en el prevalimiento es que la ventaja se exteriorice y proyecte hacia el mercado, convirtiéndose en un elemento que contribuya a modelar la forma y las condiciones en que se actúa en el mercado, en que se entra en contacto con proveedores y clientes o se establecen las relaciones con unos y otros. En el caso aquí referido, si el tratamiento ilícito de datos no afecta a las condiciones y la forma del mercado (ya sea el de intermediación publicitaria, ya sea otro) y no afecta a las relaciones con otros operadores, no se producirá dicho beneficio. Sin embargo, es destacable que la denominada «ventaja de datos» está intrínsecamente conectada al funcionamiento de los mercados digitales, permitiendo optimizar no solo la publicidad sino muchos otros servicios de las plataformas *online*. En conclusión, el aspecto crucial es si los datos obtenidos ilícitamente han sido implementados en el marco analítico de la plataforma de forma que mejoren tanto cualquiera de los servicios ofrecidos como la posición de la plataforma en cualquiera de los mercados en los que opere[71].

IV. VIOLACIÓN DE NORMAS POR COMBINACIÓN ILÍCITA DE DATOS PERSONALES CON FINES DE PUBLICIDAD PERSONALIZADA. INFRACCIÓN CUMULATIVA DE LA DMA Y DEL RGPD

1. La combinación de datos personales con fines publicitarios

Una de las principales ventajas de las que disfrutan los guardianes de acceso en comparación con otras plataformas es su capacidad para recolectar, combinar y procesar datos (personales y no personales) de sus usuarios finales a partir de la gran diversidad de fuentes que alimentan su propio ecosistema, gracias a los distintos servicios que ofrecen[72]. Los ahora denominados guardianes de acceso llevan años combinando los datos aportados por sus usuarios al registrarse con otros *rastros* que dejan dentro de su ecosistema, como el historial de navegación, las apps descargadas, la geolocalización o los vídeos y anuncios visualizados[73]. Gracias a la combinación de datos, consiguen una mayor capacidad para elaborar perfiles de sus usuarios y prestar servicios más personalizados, entre los que se incluye la pu-

[70] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318; y Emparanza Sobejano, A., «Artículo 15. Violación de normas», *op. cit.,* pp. 255-272.

[71] Estevan de Quesada, C. «Data-protection related abuses…», *op. cit.*

[72] Krämer, J., Schnurr, D. y Broughton Micova, S. «The Role of Data for Digital Markets Contestability», *CERRE Report*, 2020.

[73] Otero Cobos, M. T. «El uso de información por los guardianes de acceso sobre transacciones de terceros», en Olmedo Peralta, E. y Robles Martín-Laborda, A. (coords.), *Estudios de la red académica de defensa de la competencia (RADC)*, 2022.

blicidad[74]. Dado que la elección de los usuarios finales sobre el ecosistema en el que quieren participar es, normalmente, única, se deriva una situación de monopolio *de facto* en la captación de datos de los usuarios obtenidos a partir de una determinada categoría de servicios. Piénsese, por ejemplo, en la opción de un consumidor final por un determinado dispositivo móvil que funciona bajo un determinado sistema operativo. Esa elección ya marcará que los datos generados por el uso de dicho sistema sean apropiados por la empresa desarrolladora del mismo. Pero esta, además, extenderá su ámbito de captación a datos prestados en otros servicios vinculados con el sistema operativo a causa del efecto de ecosistema, como son los generados en el uso de tiendas de aplicaciones o de los servicios ofrecidos por defecto en el dispositivo móvil (motor de búsqueda, navegador web, etc.)[75].

Desde la perspectiva del bienestar del consumidor la personalización no tiene por qué conllevar siempre efectos negativos, pudiendo servir para mostrar contenidos de mayor interés, seleccionar los datos de mayor pertinencia y reducir el coste de búsquedas dentro del exceso de información que impera en los mercados digitales[76]. Podría decirse que facilitan una suerte de reducción de costes de transacción, tanto desde el lado del usuario como desde el lado de las empresas que quieren interactuar con él. Sin embargo, la combinación de datos puede presentar también sus riesgos para la privacidad, al permitir el rastreo (*tracking*) a través de diferentes servicios sin que los usuarios sean a menudo conscientes de ello o sin tener la opción de rechazar este seguimiento.

La posibilidad de que la combinación de datos pueda suponer una ventaja excesiva para los guardianes de acceso creando obstáculos de entrada al mercado es uno de los mayores problemas que emergen de la interacción entre la protección de datos y la defensa de la competencia en el entorno digital[77].

A nivel jurisprudencial, el principal pronunciamiento que se ha producido hasta la fecha sobre esta relación se ha emitido con relación a un caso alemán contra Facebook en el que el *Bundeskartellamt* prohibió la combinación de datos de usuarios entre los diversos servicios prestados por Meta (incluyendo Facebook, Instagram y WhatsApp) así como de aquellos datos obtenidos a partir de otras webs indexa-

---

[74] Article 29 Working Party, *Guidelines on Automated individual…, op. cit.*

[75] Olmedo Peralta, E. «Entornos Informáticos…», *op. cit.,* pp. 349-353.

[76] Botta, M. y Wiedemann, K. (2020), «To Discriminate or Not to Discriminate? Personalised Pricing in Online Markets as Exploitative Abuse of Dominance», *50 European Journal of Law and Economics*, pp. 381-404.

[77] Olmedo Peralta, E. «Colaboración en la generación, intercambio y procesamiento de datos (big data): entre la cooperación lícita y las conductas antitrust», en Ruiz Peris, J. I. y Estevan de Quesada, C. (dirs.), *Cooperación y mercados digitales*, Atelier, 2023, pp. 107-110.

das (los llamados *datos off-Facebook*)[78]. Este caso se sostuvo en un precepto de la Ley de Defensa de la Competencia alemana[79] aplicable a las *empresas de importancia primordial para la competencia en los mercados*[80], tales como Alphabet y Meta[81]. El precepto en cuestión establece que el Bundeskartellamt puede prohibir a dichas empresas crear o aumentar de forma apreciable las barreras a la entrada en el mercado, obstaculizar de otro modo a otras empresas mediante el tratamiento de datos pertinentes para la competencia que hayan sido recopilados por la empresa, o exigir términos y condiciones que permitan dicho tratamiento, en particular:

a) condicionando el uso de los servicios a la aceptación por parte del usuario del tratamiento de datos de otros servicios de la empresa o de un proveedor tercero, sin dar al usuario la posibilidad suficiente de elegir si, cómo y con qué finalidad se tratan dichos datos;

b) tratando los datos pertinentes para la competencia recibidos de otras empresas con fines distintos de los necesarios para la prestación de sus propios servicios a dichas empresas, sin dar a estas empresas la posibilidad suficiente de elegir si, cómo y con qué finalidad se tratan dichos datos[82].

El caso finalmente dio lugar a varias cuestiones prejudiciales ante el TJUE, resueltas en la ya referida sentencia *Meta v Bundeskartellamt*[83]. La dilatada duración del caso ante la jurisdicción alemana, así como la dificultad para encasillar las combinaciones de datos en cuestión dentro de las tradicionales teorías del daño del derecho *antitrust,* históricamente desarrolladas de la mano de la evolución jurisprudencial, propiciaron el desarrollo de una solución regulatoria, incluyéndose —ya a nivel comunitario— la prohibición del art. 5.2 en el texto de la DMA[84]. Procedemos seguidamente al estudio de sus implicaciones.

---

[78] Podszun, R. *Digital Markets Act…, op. cit.,* p.80-92.

[79] *Gesetz gegen Wettbewerbsbeschränkungen*, en adelante, GWB.

[80] «Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb», según se expresa literalmente en la §19.a GWB. El concepto se ha extendido también en su versión anglosajona, conociéndose como «undertakings with paramount significance for competition across-markets».

[81] Podszun, R. *Digital Markets Act…, op. cit.,* p.80-92.

[82] Sección 19.ª (2) no.4 de la GWB.

[83] Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023, asunto C-252/21, Meta Platforms y Bundeskartellamt (ECLI:EU:C:2023:537), párrafo 117.

[84] Para una visión del desarrollo jurisprudencial del daño en derecho de la competencia, véase Martí Miravalls, J. «La responsabilidad civil por infracción del derecho de la Competencia», en CEFLegal: Revista práctica de derecho. Comentarios y casos prácticos, núm. 225, 2019; Martí Miravalls, J. M. «Acciones de daños por infracción del derecho de la competencia: responsabilidad conjunta y prescripción», en *Actas de derecho industrial y derecho de autor*, tomo 37, 2016-2017.

2. Identificación de la norma vulnerada: el art. 5.2 de la DMA

Los riesgos en torno a la privacidad de los usuarios y al posible levantamiento de barreras de entrada al mercado como resultado de combinaciones de datos por parte de guardianes de acceso dieron lugar a uno de los preceptos más debatidos y criticados durante el proceso legislativo de la DMA: el art. 5.2[85]. Desde un plano formal, el precepto —al incluirse en un Reglamento de la UE— forma parte claramente del supuesto de hecho general del art. 15 LCD por razones que damos aquí por reproducidas. En sentido material, se cumplirían también los requisitos generales exigidos para su aplicación, al ser una norma reguladora de prácticas en el mercado y tener, por tanto, carácter concurrencial, como expondremos más adelante. En sentido personal, conviene recordar que la DMA solo resulta aplicable a los guardianes de acceso. En nuestro caso nos estamos refiriendo a las prácticas de Alphabet, Meta y Amazon, que han sido designadas como guardianes de acceso, pero hemos de advertir que esta prohibición no afectaría a otras posibles plataformas que no sean designadas como tales.

El precepto establece cuatro prohibiciones particulares, que pueden englobarse de forma conjunta en una prohibición general de *combinación de datos*[86]. La literalidad del precepto señala que el guardián de acceso se abstendrá de realizar lo siguiente:

a) tratar, con el fin de prestar servicios de publicidad en línea, los datos personales de los usuarios finales que utilicen servicios de terceros que hagan uso de servicios básicos de plataforma del guardián de acceso.

b) combinar datos personales procedentes de los servicios básicos de plataforma pertinentes con datos personales procedentes de cualesquiera servicios básicos de plataforma adicionales o de cualquier otro servicio que proporcione el guardián de acceso o con datos personales procedentes de servicios de terceros.

c) cruzar datos personales procedentes del servicio básico de plataforma pertinente con otros servicios que proporcione el guardián de acceso por separado, entre ellos otros servicios básicos de plataforma, y viceversa.

d) iniciar la sesión de usuarios finales en otros servicios del guardián de acceso para combinar datos personales.

---

[85] Como ejemplo de críticas al precepto durante el proceso legislativo, *vid.* Irish Council for Civil Liberties, «Greater protection in Article 5 (a) of the Commission's proposal for a Digital Markets Act», 25 de enero de 2021.

[86] Botta, M. «Compliance with the DMA obligations: the prohibition of data combination under art. 5(2) DMA», en Ruiz Peris, J. I. y Estevan de Quesada, C. *New European Competition Trends…, op. cit.,* pp. 259-280.

A pesar de que durante el proceso legislativo se llegó a proponer que dichas prohibiciones fuesen absolutas o solo decayesen cuando la combinación en cuestión fuese estrictamente necesaria, el precepto cierra estableciendo una serie de excepciones que disminuyen notablemente su ámbito operativo[87]. Estas son: el consentimiento del usuario final[88], la necesidad para el cumplimiento de una obligación legal aplicable al responsable del tratamiento[89], la necesidad para proteger los intereses vitales del interesado[90] y la necesidad para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento[91]. En lo que aquí nos atañe, que es la combinación de datos personales con fines de elaboración de perfiles publicitarios, tendrá especial relevancia el consentimiento como excepción a las anteriores prohibiciones. Ello configura al consentimiento como talón de Aquiles de esta prohibición de la DMA, proyectando también sus efectos sobre la efectividad de otros Reglamentos, como advertíamos previamente.

Las prohibiciones del art. 5.2 DMA operan como una infracción cumulativa: para que se incumpla la prohibición, no es necesario exclusivamente que se haya llevado a cabo la combinación de datos vetada, sino que, además, el consentimiento prestado por el usuario para el tratamiento de los datos personales con tales fines debe ser contrario al RGPD. Esta situación provoca una parálisis ejecutoria en la que las decisiones de la Comisión por posibles vulneraciones del art. 5.2 DMA dependerán y dependen de forma absoluta de la legalidad del consentimiento otorgado, extremo que pasa por examinar la validez de complejos sistemas de consentimiento implementados por los guardianes de acceso, como el *pay-or-okay* de Meta.

Si bien la vulneración de estas normas debe ser cumulativa, ambas infracciones deben examinarse por separado bajo la luz del art. 15 LCD. Por un lado, porque la infracción del art. 5.2 de la DMA es diferenciable de la infracción de los requisitos relativos al consentimiento bajo el RGPD. El art. 5.2 de la DMA opera como *lex specialis* respecto al RGPD, si bien se construye sobre la base del mismo. Como argumenta Bania, la expresión «sin perjuicio del RGPD» que utiliza el considerando 12 de la DMA significa que las obligaciones de la DMA se establecen sin detrimento de la normativa preexistente[92]. De ahí que en lo referente al tratamiento de datos primará el RGPD,

---

[87] Graef, I. «Why end-user consent cannot keep markets contestable», 2021, *Verfassungs Blog*.

[88] De conformidad con los arts. 4 (11) y 7 del RGPD.

[89] Art. 6 (1) *c)* RGPD.

[90] Art. 6 (1) *d)* RGPD.

[91] Art. 6 (1) *e)* RGPD.

[92] Bania, K. «Fitting the Digital Markets Act in the Existing Legal framework: the Myth of the Without Prejudice Clause» *19(1) European Competition Journal*, 2023, pp. 116-149.

mientras que la DMA operará para penalizar la combinación ilícita de datos por parte de guardianes de acceso. Esta actividad puede afectar a los objetivos de la norma: garantizar la equidad y disputabilidad de mercados digitales en los que intervengan guardianes de acceso, en beneficio de los usuarios profesionales y finales[93].

Por otro lado, como argumentábamos previamente, no debe ignorarse que las infracciones del RGPD deben examinarse bajo la modalidad de violación de normas no concurrenciales. Si el examen de la infracción cumulativa fuese conjunto, la necesidad de probar los requisitos del art. 15.1 LCD se extendería también a la infracción del art. 5.2 de la DMA. En cambio, si el examen es separado, cabe la posibilidad de que la DMA se califique como una norma concurrencial y, por tanto, se presuma el cumplimiento de tales requisitos.

3. Calificación de la norma: la DMA como norma concurrencial

Una vez identificada la norma potencialmente infringida, es necesario dilucidar si el art. 5.2 DMA presenta o no carácter concurrencial a efectos de someterla al régimen del párrafo primero o el párrafo segundo del art. 15 LCD, pues los requisitos para declarar la deslealtad de la acción son considerablemente distintos en uno y otro caso. El debate en la doctrina internacional sobre si la DMA es o no una norma concurrencial (entendida como norma *antitrust* o de competencia) puede parecer, de inicio, una mera preocupación teórica, pero guarda una relevancia práctica esencial a efectos de determinar una posible violación de normas bajo el art. 15 LCD[94].

Algunos autores sostienen que el carácter de la DMA es ambiguo, si bien reconocen que cada obligación impuesta por ella puede asociarse en cierto modo con la prevención de, al menos, una de las dos categorías de abuso de posición de dominio consideradas tradicionalmente por el derecho *antitrust*: la exclusión o la explotación[95]. Otros añaden que los objetivos de la DMA son similares a los del derecho de la competencia, si bien la forma de alcanzarlos es diferente. Mientras que la

[93] Art. 1.1 DMA.

[94] Como señalan ciertos autores, el carácter de la DMA también es relevante para determinar ciertos problemas prácticos de implementación. A título de ejemplo, si el reglamento es entendido como una norma de derecho de la competencia, debe interpretarse bajo la guía interpretativa de la jurisprudencia referente al art. 102 del TFUE. Si por el contrario es entendida como una norma *sui generis*, gozará de una mayor libertad e independencia respecto a los precedentes en derecho de la competencia. Por todos, Moreno Belloso, N. y Petit, N. «The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove», *European Law Review* 391, 2023.

[95] *Ibid.*

primera establece una serie de obligaciones *ex ante* con el objetivo de regular el funcionamiento del mercado permitiendo su disputabilidad y favoreciendo la equidad y la justicia en su funcionamiento, el derecho *antitrust* se caracteriza por abordar *ex post*[96] conductas consideradas singularmente aplicando las reglas de los arts. 101 y 102 del TFUE[97]. Por ello, la DMA sería una norma de carácter regulatorio y no de competencia[98].

A efectos del art. 15 LCD el foco no debe situarse en las posibles divergencias de método entre la DMA y el derecho *antitrust*, sino en la coincidencia en su objeto. El art. 15.2 LCD hace referencia única y expresa a normas jurídicas que tengan *por objeto la regulación de la actividad concurrencial*. En consecuencia, lo relevante no será si la DMA sigue el mismo *iter* regulatorio que el derecho de la competencia o presenta un carácter análogo a su normativa, sino si persigue el objeto de regular la actividad concurrencial. En otras palabras, el art. 15 LCD es indiferente al proceso seguido por la norma infringida, puesto que el factor determinante de la aplicabilidad de uno u otro de sus apartados es si la norma infringida tiene como objeto o no regular la actividad concurrencial. Por ello, deberemos definir como foco del debate la cuestión de definir el objeto del art. 5.2 de la DMA y no sus métodos de implementación.

La determinación del objeto del precepto potencialmente infringido pasa antes de nada por analizar su encuadre sistemático y contextual. El art. 5.2 se sitúa en el capítulo tercero de la DMA, titulado «prácticas de los guardianes de acceso que limitan la disputabilidad o son desleales». La interpretación de dicho título debe complementarse con el considerando 36 de la norma, el cual advierte del trasfondo del precepto, al señalar que la acumulación de datos por parte de guardianes de acceso crea obstáculos de entrada al mercado y menoscaba deslealmente la disputabilidad de los servicios básicos de plataforma. Desde una perspectiva teleológica, se deriva igualmente que la función última del art. 5.2 DMA —como el de toda la norma en su conjunto— es la de «contribuir al correcto funcionamiento del mercado interior estableciendo normas armonizadas que garanticen a todas las empresas, en toda la Unión, la equidad y la disputabilidad de los mercados en el sector digital donde haya guardianes de acceso, en beneficio de los usuarios profesionales y los usuarios finales»[99].

---

[96] Lógicamente dejamos fuera de esta consideración lo relativo al control de operaciones de concentración y ayudas de Estado que, a pesar de formar parte del núcleo tradicional del derecho de la competencia, implican una actuación preventiva.

[97] Reyna, A. «Why the DMA is much more than competition law (and should not be treated as such)», *Chillin'Competition*, 16 de junio de 2021.

[98] Olmedo Peralta, E. «Redefiniendo el ámbito de aplicación…», *op. cit.*; y Olmedo Peralta, E. «La construcción de un régimen jurídico…», *op. cit.*

[99] Art. 1.1 DMA.

De todo esto se entiende que el objeto general del precepto es evitar prácticas que limiten la disputabilidad o sean desleales. En este punto, el significado del término deslealtad ha sido cuestionado por algunos autores. Hoffmann advierte que, pese a que la raíz *fair* (leal[100]) aparezca 90 veces en el texto en inglés de la DMA, esta noción se utiliza en contextos muy diferentes, si bien bajo el denominador común de que la DMA distingue sistemáticamente entre este concepto y la disputabilidad del mercado (*contestable markets*). A la hora de señalar similitudes entre la DMA y el derecho de la competencia, diversos autores señalan que el término *fair* aparece también en el derecho *antitrust*. En concreto, la exención general del art. 101.3 TFUE requiere la reserva a los usuarios de una participación equitativa (*fair share*) en el beneficio resultante de una práctica colusoria. Del mismo modo, en el listado de posibles prácticas anticompetitivas, el art. 102 TFUE incluye, entre otras, la imposición directa o indirecta de condiciones de transacción no equitativas (*unfair trading conditions)*[101]. Aun así, la DMA parece estar utilizando el término *fairness* para regular algo que sobrepasa el mero concepto de justicia distributiva, abogando más bien por regular comportamientos desleales, como ejemplifican los arts. 5 y 6 de la norma[102].

Hoffmann sostiene que las divergentes traducciones del término *fair* en distintas versiones lingüísticas de la DMA parecen apuntar a que el legislador comunitario identifica este término con la equidad[103]. Así, la versión española del art. 1.1 de la DMA señala que los objetivos de la norma son garantizar la *equidad y disputabilidad de los mercados*, y otros muchos considerandos y preceptos de la DMA se refieren conjuntamente a medidas o problemas de disputabilidad o equidad[104]. El término equidad también fue el preferido en la traducción española de los referidos arts. 101 y 102 del TFUE.

De las anteriores interpretaciones se deriva que el objeto principal del art. 5.2 de la DMA es hacer frente a comportamientos (combinaciones de datos) que limiten la disputabilidad creando barreras de en-

---

[100] La traducción literal de *fair* al castellano sería la de justo o equitativo (también, razonable, adecuado o moderado). Sin embargo, por el objetivo de la norma y la tradición lingüística normativa en español, la traducción ha de hacerse de su antónimo *unfair*, que sí se traduciría más naturalmente como desleal (injusto o engañoso). En consecuencia, si *unfair* se traduce cómodamente en el ámbito en que nos encontramos como *desleal*; *fair* debe entenderse, en una terminología más adecuada a nuestra tradición normativa, como *leal*.

[101] Por todos, Bania, K. «Fitting the Digital Markets…», *op. cit.*; y Hoffmann, L. J. «Fairness in the Digital Markets Act», *European Papers,* vol. 8, núm. 1, 12 de abril 2023, pp. 17-23. Nótese que, a pesar de que el listado del 101.1 TFUE se refiere también a «fijar directa o indirectamente los precios de compra o de venta u otras condiciones de transacción», no menciona que éstas hayan de ser «no equitativas» (a diferencia del 102).

[102] Bania, K. «Fitting the Digital Markets…», *op. cit.*

[103] Hoffmann, L. J. «Fairness in the Digital Markets Act», *op. cit.*

[104] Entre otros, *vid.* considerandos (7), (8) y (28), y arts. 18 (2) y 41 (4) de la DMA.

trada y/o que sean desleales en el sentido de menoscabar la equidad en los mercados en los que intervengan guardianes de acceso[105]. Fijado este objeto, es sostenible que el art. 5.2 de la DMA revista el carácter de norma concurrencial a efectos del art. 15 LCD. Esta caracterización se encuentra en línea con la definición aportada por la doctrina española, la cual sostiene que regulan la actividad concurrencial, entre otras, aquellas normas que establecen conductas propiamente concurrenciales de los agentes que operan en el mercado, dirigidas a promover o asegurar la difusión de las prestaciones en el mercado, por ejemplo, limitando las prácticas de promoción de ventas o predeterminando el contenido de la oferta[106].

Siendo el objeto del art. 5.2 de la DMA limitar una práctica concreta (la combinación de datos con diversos fines, como los publicitarios) por parte de guardianes de acceso en los mercados digitales, lo coherente es aplicar el art. 15.2 LCD, relativo a la violación de normas concurrenciales, para determinar si la infracción del precepto en cuestión merece el reproche de deslealtad.

4. Consecuencias de tratar al art. 5.2 DMA como una norma concurrencial. La presunción del art. 15.2 LCD

Con ocasión de exponer una posible violación de normas no concurrenciales por infracción de las bases legales establecidas por el RGPD, exponíamos que, bajo el art. 15.1 LCD, no solo es necesario probar la infracción normativa, sino también la obtención de una ventaja competitiva significativa como resultado de dicha infracción y el prevalimiento de la ventaja por parte del infractor o el beneficiario. Constatado el carácter concurrencial del art. 5.2 de la DMA y la consecuente aplicabilidad del art. 15.2 LCD, la principal diferencia respecto al caso anterior es que se presumirá la concurrencia de estos requisitos, por mor del carácter concurrencial de la norma infringida. Esta presunción tiene carácter *iuris tantum*, por lo que es posible que el infractor

---

[105] Es oportuno advertir que, conforme a la interpretación de algunos autores, el art. 5 (2) DMA guarda un doble objeto: por un lado, evitar la proliferación de barreras de entrada al mercado, y por otro, proteger el derecho fundamental a la protección de datos de los usuarios finales, cuyos datos no deberían ser explotados fácilmente con fines comerciales. Como se ha advertido previamente, la DMA funciona como *lex specialis* respecto al RGPD en cuanto al tratamiento de datos personales (ya que se establece «sin perjuicio del RGPD)», por lo que entendemos que este segundo objeto (la protección de datos) es un objeto secundario, siendo el propósito principal del precepto asegurar la disputabilidad y la equidad en los mercados en los que intervienen guardianes de acceso. La posible apreciación de un doble objeto o de un objeto secundario, a nuestro entender, no es obstáculo para la declaración del carácter concurrencial de la norma a efectos del art. 15 LCD. Respecto al doble objeto del art. 5 (2) de la DMA, *vid.* Podszun, p. 81.

[106] Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730; y Massaguer Fuentes, J. «Artículo 15. Violación de Normas…», *op. cit.*

alegue como técnica de defensa que no concurre uno o algunos de los requisitos anteriormente expuestos.

La diferencia sustancial, en conclusión, es que se presume (salvo prueba en contrario) la deslealtad de la práctica cuando se constate la violación normativa. En el caso de la aplicación del modelo *pay-or-okay* por parte de Meta, si bien no existe prejudicialidad ni vinculación por el juez civil, entendemos que la decisión de la Comisión en la que sanciona a Meta por una infracción del art. 5.2 DMA puede y debe ser tenida en consideración para valorar la deslealtad de la práctica, si bien es cierto que la Comisión solo se ha pronunciado con respecto a la legalidad del primer modelo *pay-or-okay*, y no sobre aquel implementado a partir de noviembre de 2024. Con respecto a las combinaciones de datos acaecidas con posterioridad a esta fecha bajo el nuevo modelo, es previsible que el juez nacional actúe con prudencia a la espera de una decisión por parte de la Comisión Europea.

V. VIOLACIÓN DE NORMAS POR EXPLOTACIÓN ILÍCITA CONFORME A LA DSA. LA PRESENTACIÓN DE PUBLICIDAD BASADA EN PERFILES UTILIZANDO DATOS SENSIBLES

1. Identificación de la norma vulnerada. ¿Se somete la infracción del art. 26.3 de la DSA al ámbito de aplicación general del art. 15 LCD?

Como se ha considerado anteriormente, el supuesto de hecho general del art. 15 LCD presenta dos componentes: *violación* y *norma*. Hemos de considerar ahora el carácter y sumisión a esta regla de la infracción del art. 26.3 DSA, que prohíbe la presentación de publicidad basada en perfiles usando datos sensibles por parte de plataformas en línea. El análisis de la *norma* infringida ha de basarse en dos componentes: el formal y el material. La DSA cumpliría los requisitos formales al ser un Reglamento de la UE, por razones que damos por reproducidas. Respecto a la vertiente material, la respuesta requiere un mayor desarrollo.

Advertíamos que la doctrina tiende a encuadrar la violación de normas como un ilícito contra el mercado, si bien reconoce que ciertos comportamientos pueden sufrir el reproche de deslealtad por vulnerar al mismo tiempo los intereses de los consumidores y los intereses de los competidores, además de las condiciones de competencia libre y no falseada en el mercado[107]. En el caso de la prohibición de la DSA, el comportamiento reprobable no es el tratamiento o la combinación

[107] Por todos, Carbajo Cascón, F., «Violación de secretos, inducción…», *op. cit.*

ilícita de datos personales (extremos de los que ya se encargan respectivamente el RGPD y la DMA), sino que la conducta vedada es la explotación efectiva de datos personales sensibles con un fin particular: la presentación de publicidad basada en perfiles. En caso de que el prestador de una plataforma en línea vulnere esta prohibición, la infracción solo merecerá el reproche de deslealtad del art. 15 LCD si depara efectos negativos sobre el funcionamiento concurrencial del mercado y, de forma particular, sobre la posición de igualdad en que deben encontrarse todos los operadores económicos. Este efecto justifica que un ilícito externo al sistema de competencia desleal devenga asimismo ilícito internamente[108].

Al igual que en el examen anterior sobre posibles violaciones normativas por infracción del RGPD, no es conveniente excluir de inicio a la DSA del supuesto general de la norma por el mero hecho de que el precepto tenga como objeto directo proteger la esfera personal del individuo y, más en particular, su derecho a la protección de datos y a la no discriminación. Al igual que los datos personales no sensibles, los datos sensibles tienen el potencial de ofrecer una ventaja significativa para el infractor. De hecho, la conducta prohibida es utilizarlos para personalizar la publicidad, personalización que permite mejoras en el sistema de IA empleado y que resultará normalmente en una prestación del servicio publicitario más eficiente, aumentando la efectividad y el éxito del mensaje transmitido. Si bien el examen debe ser casuístico, este potencial no debe desatenderse y requiere que la infracción se examine bajo el art. 15 LCD, si bien antes deberá dilucidarse si la norma vulnerada tiene o no carácter concurrencial.

2. Calificación de la norma. La DSA como norma no concurrencial

Señala la doctrina que en el supuesto de infracción de normas no concurrenciales la reprochabilidad viene determinada por la lesión indirecta a la *par conditio concurrentium*, mientras que en el supuesto de violación de normas concurrenciales el reproche asume además la salvaguardia inmediata de las condiciones o la estructura jurídica de la competencia económica diseñada por el legislador. A efectos de determinar si el art. 26.3 de la DSA se encuadra en un supuesto o en otro, será necesario delimitar su objeto directo puesto que, como señala la jurisprudencia del TS, la norma en cuestión debe tener como

[108] En este sentido se pronuncian, por todos, Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.*; y Alfaro Águila-Real, J., «Competencia desleal por infracción de normas…», *op. cit.,* pp. 667-730.

objeto directo —y no reflejo o indirecto— la regulación de la actividad concurrencial[109].

Como se ha justificado anteriormente en mayor profundidad, el objeto directo del art. 26.3 de la DSA no es otro que proteger a los sujetos de datos frente a posibles efectos adversos derivados de la explotación de sus datos sensibles con fines de publicidad basada en perfiles, lo cual justifica que se haya optado por establecer una prohibición absoluta. Esta situación es insólita en comparación con el tratamiento o la combinación de dichos datos bajo el RGPD y la DMA, que sí prevén excepciones en sus respectivas prohibiciones, las cuales a menudo son tachadas como una debilidad para la operatividad efectiva de estas últimas. Lo reseñable de la prohibición de la DSA es que el sujeto de datos puede haber otorgado de forma válida su consentimiento para el tratamiento y/o la combinación de sus datos sensibles con fines publicitarios, pero dicha validez será irrelevante a efectos de evitar la ilicitud de la práctica publicitaria si la misma presenta los caracteres del art. 26.3 DSA.

Así las cosas, se torna necesario dilucidar casuísticamente si la presentación de publicidad basada en perfiles usando datos sensibles por plataformas en línea puede constituir una violación de normas concurrenciales en el sentido del art. 15.2 LCD. Adelantamos que el examen guarda similitudes con aquel realizado respecto a las bases ilícitas de tratamiento con fines de publicidad personalizada puesto que, a fin de cuentas, los datos sensibles no son sino una categoría especial de datos personales, compartiendo su valor económico y su potencial en términos competitivos.

3. Examen legal bajo el art. 15.1 LCD

Si bien los datos sensibles son una categoría de datos personales, presentan ciertas particularidades regulatorias bajo el RGPD y la DSA debido a su mayor potencial para producir efectos adversos. A estrictos efectos del art. 15.1 LCD esta aproximación por riesgo resulta irrelevante, puesto que el propósito del precepto es reprochar aquellas conductas que lesionen la *par conditio concurrentium*[110]. En este contexto resultará indiferente que la publicidad en cuestión perjudique los intereses o derechos fundamentales de sus destinatarios, ya que la infracción normativa solo será relevante si se exterioriza hacia el mercado.

---

[109] STS 593/2000, 16 de junio de 2000 [RJ 2000, 5288]. (Fundamento Jurídico tercero, con relación al art. 15 (2) LCD).

[110] Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318.

La cuestión es si la presentación de publicidad basada en perfiles usando datos sensibles otorga una ventaja competitiva significativa al infractor (en este caso, el prestador de la plataforma como sujeto obligado) o a un tercero beneficiario. Debe plantearse si la ventaja competitiva obtenida en el mercado es causada por el uso publicitario de datos sensibles ya que, de no tener los mismos un papel significativo, la infracción no resultaría en una violación de normas.

El presente supuesto reviste especial complejidad frente a los casos de violación de normas anteriormente planteados. Esta complejidad se manifiesta ya en el primer paso: determinar si concurre una violación de normas. La prueba de una infracción del art. 26.3 DSA se enfrenta a los diversos obstáculos que hemos considerado anteriormente. Entre ellos, destaca la necesidad de cumplir con obligaciones de transparencia respecto a los parámetros utilizados para personalizar la publicidad, obligaciones que se pueden ver mermadas cuando el obligado alegue la concurrencia de secretos comerciales esenciales sobre el sistema publicitario. Aun en el caso de que se ofrezca una mínima transparencia sobre los parámetros utilizados, se suma el inconveniente de tener que calificar los datos como sensibles o no sensibles para que opere la prohibición de la DSA. Esta calificación, como señalábamos, resulta enormemente confusa debido a los grandes problemas interpretativos que rodean al concepto de datos sensibles, heredado del RGPD.

Este primer requisito (la prueba de una infracción normativa) plantea la duda razonable de si la violación de normas es un instrumento de escasa eficacia en este contexto, ya que el mismo hereda los inconvenientes del supuesto de hecho del art. 26.3 DSA, a los que, para mayor gravedad, se suman el resto de requisitos del art. 15.1 LCD, esto es: *a)* que de la infracción se derive una ventaja competitiva para el infractor o para un tercero, *b)* que esa ventaja sea significativa y *c)* que el infractor se prevalga en el mercado de esa ventaja significativa.

El examen de estos factores deberá realizarse caso por caso, al igual que en el supuesto de violación de normas por infracción de las bases de tratamiento conforme al RGPD o a la combinación ilícita de datos bajo la DMA. Ahora bien, la prohibición de la DSA parece guardar una menor operatividad bajo el supuesto de violación de normas, debido a las excesivas incertidumbres que rodean al supuesto de hecho del art. 26.3 de la DSA, así como por la probabilidad de que la prohibición produzca un impacto excesivamente limitado en el funcionamiento del mercado (factor fundamental a efectos del art. 15 LCD). En conclusión, el supuesto queda circunscrito a categorías de datos personales que son relevantes para la protección de los derechos fundamentales, pero guardan un menor protagonismo en la *par conditio concurrentium,* por lo que la prueba de deslealtad será más compleja en estos supuestos.

VI. REFLEXIONES FINALES. PROBLEMAS APLICATIVOS DEL ILÍCITO DE DESLEALTAD DE LA VIOLACIÓN DE NORMAS AL USO DE DATOS SENSIBLES EN LA ACTIVIDAD PUBLICITARIA

Como se ha apuntado en nuestra doctrina, la violación de normas del art. 15 LCD es una norma que carece de antecedentes tanto en la legislación española sobre competencia desleal como en el derecho comparado[111]. Pese a su acotación principal al marco jurídico español, esta conducta puede resultar relevante para hacer frente a ciertas prácticas comerciales que son personalizadas sobre la base de los datos personales de sus destinatarios. Prueba de ello es sin duda la demanda de AMI a Meta por competencia desleal, o la sentencia del Tribunal de Justicia en el caso *Lindenapotheke*, en las que se advierte la necesaria complementariedad entre las infracciones del RGPD y la violación de normas como instrumento nacional para reforzar los derechos de los interesados afectados por la infracción normativa[112].

La violación de normas ya ha sido advertida como un posible instrumento para hacer frente a tratamientos ilícitos de datos personales que tengan repercusión en el funcionamiento concurrencial del mercado[113]. En el caso de la violación de normas por infracción del RGPD, el art. 15 LCD presenta como virtud que opera con independencia de la caracterización del sujeto activo de la infracción o del beneficiario de la infracción, si bien es cierto que, cuando la infracción alegada sea la DMA, el sujeto infractor debe ser un guardián de acceso, debido al ámbito personal de la propia DMA.

La LCD, además, tiene la potencialidad de ofrecer a las víctimas de una conducta desleal por vulneración de normas la posibilidad de reclamar la compensación de los daños sufridos ante tal infracción. Además, pese a la reticencia generalizada de las autoridades españolas de defensa de la competencia a utilizar este instrumento, no se debe obviar la función central que en el sistema español desarrolla el art. 3 LDC como puente de conexión entre las normas de competencia desleal y las antitrust[114]. De tener una aplicación efectiva, esta norma resultaría especialmente útil en tanto que legitima a las autoridades de competencia a promover procedimientos frente a conductas

---

[111] Si bien es cierto que la misma guarda cierta presencia en la cláusula general de prohibición de la competencia desleal alemana. En este sentido, *vid.* Massaguer Fuentes, J. «Artículo 15. Violación de normas», *op. cit.,* pp. 292-318.

[112] Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de octubre de 2024, *Lindenapotheke*, asunto C-21/23 (ECLI:EU:C:2024:846).

[113] Estevan de Quesada, C. «Data-protection related abuses…», *op. cit.,* pp. 281-303.

[114] Menéndez Menéndez, A. *La competencia desleal*, Madrid, Cívitas, 1988.

de vulneración de normas que produjesen un impacto generalizado sobre la competencia en el mercado, afectando al interés público[115].

La violación de normas también podría extenderse a recientes prohibiciones introducidas por la DMA relativas a la combinación de datos personales por parte de los guardianes de acceso, práctica que presenta particulares riesgos para la disputabilidad y la equidad de los mercados digitales. En el caso de infracciones del art. 5.2 de la DMA, la violación de normas presentaría adicionalmente como ventaja la presunción del prevalimiento de una ventaja competitiva significativa adquirida como consecuencia de la infracción, ya que la norma presenta un carácter concurrencial.

Ahora bien, aplicar el ilícito de violación de normas también se enfrenta a dificultades. En el caso del tratamiento de datos con fines publicitarios bajo el RGPD y de la combinación de datos de la DMA, ambos dependen en gran medida de la validez del consentimiento, examen que en la práctica está sujeto a un amplio margen de discrecionalidad y a una considerable nota de inseguridad jurídica. Es cierto que en el caso de modelos controvertidos (como el *pay-or-okay*) instaurados por guardianes de acceso es más probable que se determine su ilicitud[116]. La ilicitud de este consentimiento desencadenaría asimismo una posible infracción del art. 5.2 DMA si fue recabado para llevar a cabo algunas de las combinaciones de datos prohibidas por el precepto. De momento, las conclusiones preliminares de la Comisión apuntan hacia una infracción de la DMA por parte de Meta debido precisamente a la ilicitud del consentimiento prestado en su modelo *pay-or-okay.*

La virtualidad de aplicación normativa ante estos supuestos admite tres cauces de actuación. El primero de ellos se basa en la infracción del RGPD. El segundo se conduce a través de la infracción de la DMA. Finalmente, se ha de tener en cuenta la posibilidad de recurrir al art. 3 LDC para que la autoridad antitrust promueva un expediente por la infracción del art. 15.2 LCD. Ello sin perjuicio de las posibles demandas de particulares por daños con base en este último precepto. Aunque el reproche de deslealtad del art. 15 LCD no sea una sanción

---

[115] Costas Comesaña, J. «Prohibición de falseamiento de la libre competencia por actos de competencia desleal», en Bello Martín-Crespo, M. P.; Hernández Rodríguez, F. (coords.) y Gómez Segade, J. A. (pr.), *Derecho de la libre competencia comunitario y español*, 2009, pp. 213-232; así como Díez Estella, F. «El art. 3 LDC: falseamiento de la competencia por actos desleales», en Beneyto Pérez, J. M. y Maillo González-Orús, J.(dirs.), *Tratado de derecho de la competencia: Unión Europea y España*, vol. 1, tomo 1, 2017, pp. 505-553. No debe ignorarse que a efectos del art. 3 LDC sí concurriría el deber de colaboración entre las autoridades de competencia y las autoridades de protección de datos al que se refiere la Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023, asunto C-252/21, *Meta Platforms y Bundeskartellamt* (ECLI:EU:C:2023:537), párrafo 117.

[116] EDPB, *Opinion 08/2024 on Valid Consent In The Context Of Consent Or Pay Models Implemented By Large Online Platforms*, 2024.

añadida a la prevista por la norma vulnerada, el hecho de que la violación de normas requiera en este caso de una infracción cumulativa previa (RGPD-DMA) guardaría un efecto punitivo excesivo en estos supuestos.

Dejando de lado las posibles infracciones del RGPD y de la DMA, en el caso de la publicidad regulada por el art. 26.3 de la DSA, la violación de normas puede plantearse como un recurso insuficiente a causa de los múltiples inconvenientes que plantea el supuesto de hecho de la norma infringida, así como la necesidad adicional de probar los requisitos del art. 15.1 LCD. En este sentido, tal vez resultaría más aconsejable acudir a otras vías que sean indiferentes tanto al concepto de datos sensibles como a la necesidad de que la práctica afecte al comportamiento de los competidores en el mercado. Siguiendo con posibles soluciones aportadas por el derecho de la competencia desleal, una alternativa podría ser su tratamiento como prácticas comerciales desleales en relación con los consumidores y usuarios, cuestión que analizaremos en el siguiente capítulo.

CAPÍTULO V

LAS PRÁCTICAS COMERCIALES BASADAS EN PERFILES QUE EXPLOTEN VULNERABILIDADES DEL DESTINATARIO. REPROCHE DE DESLEALTAD BAJO LA MODALIDAD DE PRÁCTICAS AGRESIVAS Y BAJO LA CLÁUSULA GENERAL

I. LA RELACIÓN DE COMPLEMENTARIEDAD ENTRE LA DPCD, EL RGPD Y LA DSA

En el momento de transposición de la DPCD al ordenamiento jurídico español, el impacto de la publicidad basada en perfiles todavía tenía una incidencia moderada, tanto por los medios de comunicación empleados como por los recursos disponibles para su personalización. Si bien medios de comunicación como el teléfono móvil, el fax, el correo electrónico o los mensajes de texto ya permitían en su momento un contacto directo y a distancia con los destinatarios del mensaje publicitario, estos medios no eran tan persuasivos ni eficaces como los actuales. Como adelantábamos, en la actualidad es frecuente que la publicidad basada en perfiles se presente en servicios con gran adherencia para los usuarios, como las redes sociales y los videojuegos *online*. Esta dependencia (incluso, a veces, adicción) sobre el servicio principal puede reflejarse asimismo en los resultados de la publicidad inserta en el servicio en cuestión. Por otro lado, la evolución de la publicidad personalizada no solo se aprecia en los medios utilizados para

su difusión, sino también en los recursos empleados para su personalización. Gracias al análisis de *big data* y al uso de complejos sistemas algorítmicos y de IA es posible predecir con un alto nivel de fiabilidad el comportamiento y los intereses de cada destinatario concreto.

En el momento de transposición de la Directiva este tipo de publicidad tenía una relevancia mucho menor que en la actualidad. La similitud más cercana podemos encontrarla en lo que en su momento se denominaba «publicidad directa» o «*marketing* directo». Ciertos autores distinguían tras la transposición de la DPCD al marco español dos categorías principales de publicidad: la publicidad mecanizada, que es aquella dirigida a la gran masa de consumidores, y la publicidad o marketing directo, que se dirige en cambio a cada consumidor en concreto y de una manera individualizada[1]. Es en esta segunda categoría donde se encuadraría lo que hoy entendemos como publicidad basada en la elaboración de perfiles, cuya amplia conceptualización engloba tanto los perfiles individuales como los perfiles grupales.

En el momento de transposición de la Directiva se comenzaban a apreciar las ventajas de la publicidad directa (hoy publicidad basada en perfiles) al permitir una previa selección de consumidores que, en principio, podían estar más interesados en los servicios o productos en cuestión, con el consiguiente ahorro de dinero y esfuerzo por parte del empresario y el incremento del efecto persuasivo de la publicidad[2]. Ya se advertía que, aunque toda publicidad genera cierto grado de molestia en el consumidor, en la publicidad directa puede originarse un grado de molestia adicional derivado en parte de la invasión de ámbitos propios de su esfera privada, por lo que se empezó a categorizar a la misma en el concepto de «publicidad molesta», categoría que tradicionalmente ha venido mereciendo un reproche de deslealtad en ordenamientos jurídicos como el alemán bajo la cláusula general[3].

En el caso de la publicidad basada en perfiles elaborados conforme a los datos personales del destinatario, esta invasión de la esfera privada es todavía más evidente, al afectar conjuntamente a los derechos a la privacidad y a la protección de datos. Señalaban ya en 1890 Warren y Brandeis, al definir la privacidad, que todo individuo tiene el derecho general a que le dejen en paz (*the right to be let alone*)[4], argumento que es extensible a aquellos casos en los que la explotación

---

[1] Tato Plaza, A. *et al.,* «Prácticas agresivas», en Tato Plaza, A. Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia…, op. cit.,* pp. 62-63.

[2] *Ibid.*, pp. 65-66.

[3] Tato Plaza, A. en referencia a Schricker, G. «Situación actual y evolución del derecho de la publicidad en la República Federal de Alemania», en Lema Devesa, C. (dir.) *Problemas actuales del derecho de la publicidad: Primeras Jornadas Internacionales de Derecho de la Publicidad*, Instituto Nacional de Publicidad, 1984, p.221.

[4] Warren, S. D. y Brandeis, L. D. «The Right to Privacy», *4 Harvard Law Review 193,* 1890.

de datos personales afecta al comportamiento económico del consumidor, tutelado bajo el reproche de deslealtad[5]. Subrayan ciertos autores que cuando la publicidad alcanza un grado tal de molestia que impida al consumidor una prueba sosegada y objetiva de la oferta, concurre el riesgo de que este adquiera el producto o servicio ofertado simplemente para liberarse de aquella molestia[6].

Tampoco podemos dejar de advertir que, aunque la publicidad molesta y el derecho a la privacidad guarden amplios denominadores comunes, no toda publicidad basada en perfiles resulta molesta[7]. Y, en caso de serlo, la causa de la molestia no radica necesariamente en el hecho de que la publicidad se construya sobre datos personales del usuario[8]. Partiendo de que toda publicidad es molesta en cierto grado, el reproche de deslealtad hacia la publicidad basada en perfiles puede sostenerse no en el riesgo de que el consumidor adquiera el producto para liberarse de la molestia, sino en la especial merma de su libertad de decisión como consecuencia directa de la explotación de sus datos personales.

Esta perspectiva se refleja en la actual configuración del concepto de práctica agresiva formulada por la DPCD —y acogida por la LCD—, en la cual entroncan no solo los supuestos clásicos de publicidad molesta, sino también otros casos pertenecientes a categorías diferentes[9]. Si bien en la publicidad basada en perfiles pueden concurrir elementos clásicos de deslealtad (como el acoso caracterizador del *spam),* concurren situaciones en las que el reproche de deslealtad por agresividad se funda en elementos ajenos a la molestia para el consumidor[10]. Se ha sostenido que la molestia no debe constituir el elemento único que sostenga el reproche de deslealtad, en vista de que aquellas prácticas comerciales que causen una mera molestia o incomodidad, pero

---

[5] Tato Plaza, A. *et al.,* «Prácticas agresivas…», *op. cit.*

[6] *Ibid.*, pp. 67-69.

[7] Vázquez Ruano, T. «El *spam* y la nueva regulación de la Ley de Competencia Desleal» *Revista de Derecho Mercantil, n*úm. 277, 2010, pp. 1098-1100.

[8] A título de ejemplo, un anuncio basado en perfiles puede resultar molesto por enviarse de forma persistente y sin el consentimiento del destinatario (*spam*). El anuncio también puede resultar molesto cuando el mensaje se basa en búsquedas previas sobre un determinado producto. Si tras la búsqueda el destinatario es continuamente expuesto a anuncios sobre el producto en cuestión, esta personalización puede resultar molesta (por ejemplo, si el producto ya ha sido adquirido) pero también útil, dependiendo del contexto. En ciertas ocasiones, sin embargo, es posible que los datos personales del usuario no resulten en una publicidad molesta, sino en prácticas distintas, como la personalización de precios o la exclusión de determinados destinatarios de algunas campañas. Estos escenarios se apartan del concepto tradicional de publicidad molesta, ya que solo concurre el riesgo general de afectar a la libertad de decisión, pero no el riesgo concreto de que el consumidor adquiera un producto determinado para librarse de la molestia.

[9] Massaguer Fuentes, J. «Principios generales», en Massaguer Fuentes, J. *El nuevo derecho contra…, op. cit.,* pp. 33-52.

[10] Vázquez Ruano, T. «Aproximación jurídica al *spam* desde la protección de datos de carácter personal» *Revista de la contratación electrónica*, núm. 33, 2002, pp.44-45.

no sean objetivamente capaces de alterar la decisión del consumidor medio no deberían calificarse como agresivas[11].

En otras palabras, es reseñable que el posible reproche de deslealtad frente a prácticas agresivas se orienta no a proteger a los destinatarios frente a meras molestias, sino a protegerlos frente a prácticas que pongan en riesgo su libertad de decisión. Viendo la estrecha relación entre la libertad de elección del consumidor y la explotación de datos personales, es razonable que se haya señalado la necesaria complementariedad entre la normativa de protección de datos y la normativa reguladora de las prácticas comerciales desleales[12], dado que ambas ramas tienen un fundamento común, definido en términos generales como la protección de la autonomía del individuo[13].

Al mismo tiempo, se ha señalado que el fin general perseguido por el infractor al desarrollar prácticas que vulneran ambas normas es el mismo: el económico. La búsqueda de un mayor éxito en su actividad comercial —y, por ende, de un mayor beneficio— es el motivo central que justifica el tratamiento de datos y el diseño de servicios publicitarios basados en perfiles de usuarios. Desde el plano teleológico, el objetivo primario perseguido no es el de vulnerar derechos fundamentales, sino que tales vulneraciones se producen a resultas de una actuación comercial —quizá— excesivamente agresiva[14]. La Comisión Europea sigue esta consideración en su Guía de 2021 sobre la DPCD, al señalar que, aunque el tratamiento ilícito de datos personales no desemboca automáticamente en la deslealtad de la práctica comercial, la violación del RGPD debe ser un requisito a tener en cuenta especialmente en aquellos casos en los que los datos hayan sido tratados con fines comerciales, como la elaboración de perfiles publicitarios[15]. Así las cosas, la motivación económica parece ser el hilo conductor en aquellas prácticas comerciales basadas en la explotación de datos personales.

---

[11] Fernández Carballo-Calero, P. «Aggressive Commercial Practices in the Case Law of EU Member States» in *Journal of European Consumer and Market Law*, vol. 5, núm. 6, 2016, pp. 255-261.

[12] Hacker, P. «Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law», *European Law Journal,* 2021, pp. 30-32; Van Eijk, N., Jay Hoofnagle, C. y Kannekens, E., *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, 2017, p.12; y Trzaskowski, J., «Persuasion, Manipulation, Choice Architecture and 'Dark Patterns» in Savin, A. y Trzaskowski, J., *Research Handbook on EU Internet Law*, 2023, pp. 200-203.

[13] Bennis, S. «AI and the Consumer», en Savin, A. y Trzaskowski, J. (eds.), *Research Handbook on EU…», op. cit.,* pp. 482-485.

[14] *Ibid.*, pp. 461-464. El aliciente económico guarda un especial protagonismo en la publicidad *online*, cuyo mercado global fue valorado en 319 billones de dólares en 2019 y se espera que alcance los 1,089 billones de dólares en 2027. Allied Market Research, «Internet Advertising Market Statistics, 2020-2027».

[15] Comisión Europea, *Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior*, 2021, p. 19.

Desde un punto de vista práctico, la normativa de prácticas comerciales desleales también puede ser un instrumento para perseguir prácticas concurrenciales injustas no sancionadas por la normativa de protección de datos, a menudo excesivamente aséptica en cuanto a los usos o consecuencias particulares del tratamiento de datos personales. En aquellos casos en los que los datos hayan sido tratados lícitamente pero su explotación concreta perjudique al comportamiento económico del consumidor, las normas nacionales de competencia desleal que se hayan desarrollado en transposición de la DPCD pueden presentarse como una alternativa para paliar ciertas prácticas merecedoras del reproche de deslealtad.

Por otro lado, conviene advertir que la normativa de prácticas comerciales desleales también puede ser un medio para abordar las lagunas de la prohibición del art. 26.2 de la DSA, expuestas en extenso anteriormente. Tanto la DPCD como la LCD tienen un ámbito subjetivo de aplicación mucho más amplio que aquella, al no limitarse a los prestadores de plataformas en línea. Igualmente, los supuestos de hecho acogidos por el reproche de deslealtad son, en cierto sentido, más flexibles que el de la prohibición de la DSA, ya que los actos desleales englobados no encuentran la limitación de remitirse al concepto de datos sensibles. Lo mismo sucede en el caso de las diversas combinaciones de datos prohibidas por la DMA, cuyo ámbito de aplicación se restringe a los guardianes de acceso.

Así las cosas, conviene estudiar si la normativa de prácticas comerciales desleales puede ser una vía para remediar prácticas comerciales que sean problemáticas sin incumplir el RGPD, la DMA o la DSA. La racionalidad de todas estas normas persigue objetivos comunes y ha de entenderse que presentan relaciones de complementariedad, como confirma *el Fitness Check* 2024[16]. A estos efectos se plantea la cuestión de si la DPCD sigue siendo adecuada para su propósito, puesto que en su año de publicación (2005) la publicidad digital basada en perfiles se encontraba mucho menos desarrollada debido a la menor cantidad de datos personales disponibles y a la inferioridad de medios técnicos para su análisis. Dada su menor utilización técnica y su menor impacto sobre el mercado, pudiera resultar que la solución de los problemas derivados de la publicidad personalizada no fuese prioritaria para el legislador comunitario en aquel momento. De ahí que no incluyese instrumentos específicos para hacer frente a su problemática. El examen de deslealtad que realizaremos a continuación tratará de abordar este interrogante.

[16] Whittle, M. *et al., Study to support the Fitness Check…, op. cit.,* p. 51.

II. EL ÁMBITO DE APLICACIÓN DE LA DPCD Y LA LCD

Antes de proceder a someter la publicidad basada en perfiles a un examen de deslealtad bajo la normativa de competencia desleal, conviene concretar el ámbito de aplicación de las normas aplicables. A nivel de la UE la DPCD es la norma que establece el marco jurídico básico aplicable a las prácticas comerciales desleales. La Directiva se transpuso al ordenamiento jurídico español a través de una modificación de la LCD. De este modo, las nuevas normas sobre prácticas comerciales se integraban dentro de los asentados precedentes de los que ya disfrutaba la normativa de competencia desleal en nuestro país y en otros del entorno[17]. La transposición de la Directiva produjo cambios mayores en el contenido y la propia definición del ámbito aplicativo de la competencia desleal[18]. En línea con la iniciativa de la UE destinada al control de adecuación de la normativa sobre competencia desleal con la legislación europea en materia de protección de los consumidores, el presente apartado se ocupará no solo del examen de deslealtad bajo la LCD, sino que también incluirá referencias a la DPCD[19]. El objeto de esta doble visión es analizar si la norma comunitaria es adecuada para hacer frente a ciertas prácticas comerciales personalizadas que resultan problemáticas en la actualidad, presentando como ventaja adicional la resolución de dudas interpretativas que puedan surgir bajo la literalidad de la LCD.

1. El ámbito de aplicación personal. Divergencias entre la DPCD y la LCD

La doctrina ya advirtió en su momento de las profundas fragmentaciones que sufrió la LCD como consecuencia de su adaptación a la DPCD[20]. Esta fragmentación se aprecia en la propia definición

---

[17] Minervini, E. y Rossi Carleo, L. *Le pratiche commerciali sleali: direttiva comunitaria ed ordinamento italiano*, A. Giuffrè, 2007; Lema Devesa, C. y Fernández Carballo-Calero, P. «La represión de la competencia desleal», en Jiménez Sánchez, G. J. y Díaz Moreno, A. (coords.), *Derecho Mercantil: vol. 2. Derecho industrial. Propiedad industrial. Explotación empresarial de la propiedad intelectual. Régimen jurídico de la competencia*, 2013, pp. 235-256; Tato Plaza, A. «Líneas generales de la reforma del derecho español contra la competencia desleal (Parte I)», *Autocontrol*, núm. 149, 2010, pp. 7-14.

[18] Miranda Serrano, L. M. «Algunas cuestiones controvertidas de las relaciones entre la normativa contractual de consumo y la reguladora de las prácticas desleales contra los consumidores», *La Ley mercantil*, núm. 110, 2024; y Tato Plaza, A. «Líneas generales de la reforma…», *op. cit.,* del derecho español contra la competencia desleal (Parte II)», *Autocontrol*, núm. 150, 2010, pp. 9-14.

[19] European Commission, *Call for evidence: Digital fairness – fitness check on EU consumer law*, 2022 y Whittle, M. *et al., Study to support the Fitness Check of EU…, op. cit.,* p. 51.

[20] Tato Plaza, A. *et al.,* «Introducción», en Tato Plaza, A. Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia…», op. cit.,* pp. 29-30.

del ámbito de aplicación personal de ambas normas, que diverge notablemente. La DPCD se aplica exclusivamente a las prácticas comerciales de las empresas en sus relaciones con los consumidores (ámbito B2C)[21]. La noción del consumidor aplicable a estos efectos como sujeto pasivo de la práctica comercial es definida por la propia Directiva como cualquier persona física que, en las prácticas comerciales reguladas, actúe con un propósito ajeno a su actividad económica, negocio, oficio o profesión. Por su parte, se considera al comerciante como sujeto activo de estas conductas, caracterizándolo funcionalmente como cualquier persona física o jurídica que, en las prácticas comerciales contempladas por la Directiva, actúe con un propósito relacionado con su actividad económica, negocio, oficio o profesión, así como cualquiera que actúe en nombre del comerciante o por cuenta de este[22]. Aunque a efectos de la Directiva debe entenderse que las nociones de comerciante y empresario son equivalentes, ciertos autores señalan que en la traducción española hubiera sido más ventajoso acudir al concepto de empresario, ya que el término comerciante no era el que, por la raigambre que tiene en el derecho mercantil español y las discusiones que había suscitado en este ámbito, hubiera sido preferible[23].

A resultas de una transposición complicada de la Directiva, el ámbito de aplicación personal de la LCD es mucho más complejo[24]. Tras la reforma de 2009, el ámbito de aplicación subjetivo de la LCD no se limita a las relaciones B2C entre empresario y consumidor —ámbito restringido de la normativa transpuesta—, sino que se aplica a los empresarios, profesionales y a cualesquiera otras personas físicas o jurídicas que participen en el mercado[25]. Esto es, a las prácticas B2B ya consideradas por la normativa, se añaden las B2C a resultas de la transposición de la Directiva.

Este ámbito personal hila con ciertas diferencias en cuanto a la finalidad de la norma. Si bien la función de la LCD es «proteger la competencia en interés de todos los que participan en el mercado»[26],

---

[21] Conforme al art. 3 (1) DPCD «La presente Directiva será aplicable a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores según establece el art. 5, antes, durante y después de una transacción comercial en relación con un producto».

[22] Art. 2 DPCD, apartados *a)* y *b)* respectivamente.

[23] Massaguer Fuentes, J. «Ámbito de aplicación de la Directiva», en Massaguer Fuentes, J. «*El nuevo derecho contra…, op. cit.,* p. 24.

[24] Señalaban Tato Plaza y otros autores que la Directiva provocó una ruptura de la unidad estructural del derecho español contra la competencia desleal, poniendo como ejemplo precisamente la divergencia entre el ámbito de aplicación del art. 3 de la Directiva (las prácticas desleales de las empresas en sus relaciones con los consumidores) con aquel de la redacción original de la LCD, que en su art. 1 señalaba (y continúa señalando) que la Ley tiene por objeto «la protección de la competencia en interés de todos los que participan en el mercado». Tato Plaza, A. *et al.,* «Introducción», *op. cit.,* p.56.

[25] Art. 3.1 LCD.

[26] Art. 1 LCD.

la DPCD circunscribe su objeto a «contribuir al buen funcionamiento del mercado interior y alcanzar un elevado nivel de protección de los consumidores»[27], es decir, mientras que la LCD pone su foco en la protección de la competencia, la DPCD se centra en la protección de los consumidores. Esta divergencia puede salvarse en cierta medida bajo una interpretación funcional del conjunto de la LCD, ya que, como señala la doctrina, la norma tiene por objetivo también, y al mismo tiempo, la salvaguardia de la libertad individual al ejercicio de la actividad económica en el mercado, de la libertad de elección de los consumidores y del derecho de todos a la formación de las relaciones de mercado según el modelo operativo propio de la competencia económica[28].

Ahora bien, conviene aclarar que la LCD incluye una lista negra o catálogo de prácticas que se consideran siempre y en todo caso desleales, pero la misma se aplica exclusivamente a las relaciones entre empresarios y consumidores. Es decir, aunque el ámbito general de la LCD se aplique a empresarios, profesionales y a cualesquiera otras personas físicas o jurídicas que participen en el mercado (incluyendo, por tanto, relaciones B2B y B2C), la lista negra solo opera para las relaciones B2C. En el resto de los casos, para examinar la deslealtad de la práctica, habrá que atender al examen general de deslealtad. De esta forma, si la práctica media en una relación B2B, deberá examinarse si la práctica es agresiva o engañosa y, en su defecto, considerar la cláusula general de deslealtad, pero no operará la presunción de deslealtad de la lista negra, aun si la práctica se enmarcase en su marco material, como puede ser el spam.

En su regulación concreta de las prácticas comerciales contra los consumidores, como advertíamos, el capítulo III de la LCD acoge la llamada *lista negra* del anexo I de la DPCD, que establece un elenco cerrado de prácticas engañosas y prácticas agresivas que se consideran desleales en cualquier circunstancia[29]. Con esta salvedad, los demás actos de competencia desleal regulados por la LCD en su capítulo II tienen un ámbito de aplicación mucho más amplio que el de la Directiva, al aplicarse con independencia de quiénes sean sus destinatarios o sujetos pasivos, esto es, tanto cuando las conductas se dirijan a los consumidores como cuando se dirijan frente a otros empresarios[30].

---

[27] Art. 1 DPCD.

[28] Massaguer Fuentes, J. *Comentario a la ley de competencia desleal*, Civitas, 1999, p. 64 ss.

[29] Miranda Anguita, A. «La letra pequeña de la publicidad ante el derecho de la competencia desleal», en Miranda Serrano, L. M. y Pagador López, J. (dirs.), *Desafíos del regulador mercantil…, op. cit.,* pp. 507-509.

[30] Este capítulo integra preceptos regulados en la DPCD (como la cláusula general o la conceptualización de las prácticas agresivas o engañosas), pero mantiene preceptos no relacionados con la Directiva al ser previos a esta, como es el caso del art. 15 LCD (regulador de la violación de normas), que se analizaron en apartados anteriores.

Así las cosas, si la práctica en cuestión se encuentra en la *lista negra* del capítulo III de la LCD solo será desleal *per se* si se dirige hacia consumidores o usuarios[31]. Si la práctica no está integrada en este catálogo o si los destinatarios en cuestión no son consumidores, se deberá acudir al examen general de deslealtad del capítulo II, que es aplicable con independencia de si los destinatarios son o no consumidores.

2. El ámbito de aplicación material. La publicidad basada en perfiles bajo los conceptos de acto de competencia desleal (LCD) y práctica comercial (DPCD)

2.1. *Consideraciones generales*

Una vez aclarado el ámbito de aplicación personal, conviene detenernos a examinar el ámbito material de la normativa reguladora de las prácticas comerciales desleales, con el objeto de determinar si la publicidad basada en perfiles está amparada por dichas normas. Se debe tener presente que el concepto de *publicidad basada en perfiles* guarda un significado propio bajo el art. 26 de la DSA (precepto de referencia en este trabajo) como fruto de la reformulación del concepto de publicidad.

Como se ha razonado anteriormente, los términos «anuncios» o «publicidad» utilizados por la DSA se alejan de la normativa precedente, al no requerir una conexión con el comercio, empresa o similar, así como por no exigirse expresamente que, a través de ellos, se persiga el objetivo de promover la contratación[32]. Esta reformulación implica, por ejemplo, que los mensajes transmitidos por las ONGs o la publicidad política tengan la consideración de publicidad a efectos de la DSA si se presentan por una plataforma a cambio de una remuneración específica[33].

A efectos del reproche de deslealtad, debemos apartarnos del concepto de publicidad de la DSA debido a que el mismo se circunscribe a la DSA, cuyo ámbito de aplicación personal y material es evidentemente distinto a aquel de la DPCD y de la LCD. Mientras que el

---

[31] Miranda Serrano, L. M. y Pagador López, J. «Misleading and Aggresive Commercial Practices and Defects of Transactional Consent», en Schulze, R. y Perales Viscasillas, M. del P. (coords.), *The Formation of Contract: New Features and Developments in Contracting*, 2016, pp. 89-9.

[32] Así, el art. 3.*r)* de la DSA define el término publicidad como «la información diseñada para promocionar el mensaje de una persona física o jurídica, con independencia de si trata de alcanzar fines comerciales o no comerciales, y presentada por una plataforma en línea en su interfaz en línea a cambio de una remuneración específica por la promoción de esa información».

[33] Duivenvoorde, B. y Goanta, C. «The regulation of digital advertising…», *op. cit.,* pp.5-13.

art. 26.3 de la DSA se aplica solo a la publicidad emitida en plataformas en línea, ni la DPCD ni la LCD presentan esta excesiva acotación. Por ello, nuestra norma patria puede considerarse una vía deseable para paliar las lagunas del ámbito personal del art. 26.2 de la DSA. Por otro lado, ciertas prácticas englobadas en el concepto de publicidad de la DSA (como la publicidad política) no se encuentran amparadas por el ámbito material de la DPCD y la LCD, al carecer de una finalidad económica o empresarial. La reformulación del término publicidad debe por tanto acotarse al ámbito para el que fue diseñada: la DSA, sin que se pueda extender a otros ámbitos normativos. En consecuencia, a efectos de este razonamiento, se debe abandonar el concepto de publicidad de la DSA para acoger —de forma genérica— las prácticas comerciales consideradas bajo el supuesto de hecho de deslealtad de la DPCD y la LCD que se basen, eso sí, en la elaboración de perfiles, ya sean estos individuales o grupales[34].

El ámbito de aplicación material de la DPCD se dirige a las prácticas comerciales desleales que perjudiquen los intereses económicos de los consumidores[35]. Señala la Directiva que una práctica comercial es «todo acto, omisión, conducta o manifestación, o comunicación comercial, incluidas la publicidad y la comercialización, procedente de un comerciante y directamente relacionado con la promoción, la venta o el suministro de un producto a los consumidores»[36]. Se ha señalado así que las prácticas comerciales quedan definidas en términos preponderantemente objetivos y funcionales, mediante dos elementos: *a)* una relación de las actuaciones en las que pueden consistir (actos, omisiones, conductas o manifestaciones y comunicaciones comerciales, incluidas la publicidad y la comercialización), y *b)* su ulterior individualización por medio de la especificación del efecto práctico relevante en este contexto (la relación directa con la promoción, venta o suministro de productos)[37].

En cuanto al aspecto objetivo, destaca la expresa inclusión de la publicidad como un subgénero dentro de las prácticas comerciales. Este extremo es subrayado por la propia DPCD, que al definir el concepto de prácticas comerciales se refiere a «todo acto, omisión, conducta o manifestación, o comunicación comercial, *incluidas la publicidad* y la comercialización, procedente de un comerciante y directamente

[34] Resulta conveniente conservar aquí el concepto de elaboración de perfiles debido a que la amplitud de este permite englobar una vasta cantidad de prácticas personalizadas que pueden resultar problemáticas para la efectiva protección de la libertad de decisión de los individuos. Recordemos que tanto el art. 26 (2) DSA como el art. 4 (4) RGPD definen la elaboración de perfiles como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física».

[35] Art. 1 DPCD.

[36] Art. 2 *d)* DPCD.

[37] Massaguer Fuentes, J. «Ámbito de aplicación de la Directiva», *op. cit.,* pp. 17-18.

relacionado con la promoción, la venta o el suministro de un producto a los consumidores»[38]. Con respecto al concepto de publicidad, la misma queda definida en el marco regulatorio de la UE por el considerando 14 de la DPEPC como «toda forma de comunicación realizada en el marco de una actividad comercial, industrial, artesanal o liberal con el fin de promover el suministro de bienes o la prestación de servicios, incluidos los bienes inmuebles, los derechos y las obligaciones», si bien (a diferencia de la DPCD) la misma se limita al ámbito B2B[39]. Por su parte, el *Libro Verde sobre Comunicaciones Comerciales* indica que la publicidad engloba el marketing directo, el patrocinio, la promoción de ventas y las relaciones públicas[40].

Respecto al aspecto funcional, ciertos autores abogan por una interpretación flexible del concepto de prácticas comerciales, afirmando que el precepto no exige que la actividad examinada tienda directamente a promover la contratación de un producto, acomodando también aquellas prácticas (como la de relaciones públicas o la actividad corporativa) que, aun cuando no promuevan directamente la contratación, están directamente relacionadas con la promoción y venta de los productos de la empresa cuya imagen se promueve[41]. Esta aproximación se confirma por las consideraciones de la propia DPCD acerca de prácticas tales como el *product placement*, la diferenciación de marcas o las acciones de promoción de ventas, cuyo sometimiento a la Directiva se asume en aquellos casos en los que pueda distorsionar el comportamiento económico de los consumidores[42].

Advierten los mismos autores que el término «venta» del precepto debería entenderse como equivalente al de «contratación», puesto que lo contrario derivaría en la exclusión (a nuestro entender ilógica) de aquellos casos en los que el empresario actúa como adquirente y no como vendedor, siendo este el caso de las campañas promocionales de empresas que se dedican a la compra y venta de productos usados. En su Guía de 2021 sobre la DPCD, la Comisión interpreta, sin embargo, que la DPCD no abarca aquellas situaciones en las que los comerciantes compran productos a los consumidores[43].

---

[38] Art. 2 *d)* DPCD, énfasis añadido.

[39] Artículo 2 *a)* de la DPEPC.

[40] Comisión Europea, *Libro Verde sobre Comunicaciones Comerciales en el Mercado Interior*, 1997, p. 9.

[41] Tato Plaza, A. *et al.,* «Introducción», *op. cit.,* pp. 30-32. Advierten los mismos autores que la lista negra de la Directiva incluso llega a incluir como desleales *per se* ciertos actos que no guardan relación directa con la venta o promoción de un producto, sino que se encaminan más a promocionar la imagen de una empresa, como es el caso de afirmar ser signatario de un código de conducta sin ser este extremo cierto (anexo I, punto 1 de la DPCD).

[42] Massaguer Fuentes, J. «Ámbito de aplicación de la Directiva», *op. cit.,* pp. 17-18.

[43] Comisión Europea, *Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales*

Ahora bien, el razonamiento de los anteriores autores se mantiene viable y no queda excluido de la interpretación (no vinculante) que realiza la Comisión a través de la Guía, al admitir posibles excepciones en las que, aunque el comerciante actúe como adquirente, pueda establecerse un vínculo entre la venta de un producto por el consumidor al comerciante y la promoción, venta o suministro de un producto (diferente) al consumidor, ofreciendo como ejemplo los acuerdos de permuta en el sector automovilístico o la compra y reventa de oro.

A nuestro entender, el concepto de práctica comercial también engloba aquellos contextos en los que el producto promocionado o anunciado es un servicio de intermediación entre vendedores y adquirentes, resultando irrelevante que los vendedores sean empresas o consumidores[44]. Como el término «producto» empleado por el precepto acoge tanto los bienes como los servicios (incluidos los inmuebles, derechos y obligaciones)[45], la publicidad sobre servicios de intermediación no debe excluirse del concepto de práctica comercial, puesto que cumple con el requisito funcional de promover la contratación de un servicio[46].

Sentado el ámbito material de la DPCD, es necesario delimitar esta misma cuestión con respecto a la LCD, al ser la norma sobre la cual se operó su transposición. Al igual que en el caso del ámbito subjetivo, es reseñable que nos encontramos ante un ámbito mucho más amplio que el de la Directiva, al prohibir los actos de competencia desleal en los que, eso sí, se enmarcan las prácticas comerciales desleales hacia los consumidores. El ámbito objetivo de la LCD difiere así de aquel de la Directiva, al aplicarse a los actos de competencia desleal, cuya conceptualización es diferente al concepto de práctica comercial. Para recaer bajo el ámbito de aplicación de la LCD, los actos de competencia desleal deben presentar las siguientes características generales: *a)* su realización en el mercado, *b)* su realización con fines concurrenciales, y *c)* ser realizados antes, durante o después de una operación comercial o contrato, independientemente de que este llegue a celebrarse o no[47].

Comenzando por la primera característica (su realización en el mercado), entienden la jurisprudencia y la doctrina que el término mercado se refiere al espacio institucional en el que se encuentran

---

desleales de las empresas en sus relaciones con los consumidores en el mercado interior, 2021, pp. 20-22.

[44] Lo que integraría tanto casos de transacciones B2B, B2C, o C2C, ya sea de productos nuevos o de segunda mano (véase como ejemplo los servicios de Vinted o Wallapop).

[45] Art. 2 *c)* DPCD.

[46] A título de ejemplo, un anuncio sobre Wallapop no dejaría de ser una práctica comercial en el sentido de la DPCD, puesto que se está promocionando un servicio, con independencia de que aquellos que ofrecen sus productos en Wallapop sean o no comerciantes.

[47] Art. 2, apartados (1) y (2) LCD.

oferta y demanda, en el que se forman y desenvuelven las relaciones económicas[48]. Como consecuencia de ello, el ámbito de la norma se extiende a todas las actividades económicas en sentido amplio (cualquiera que sea la iniciativa y la finalidad a que obedezcan), entre las que se cuentan no solo las actividades empresariales (civiles y mercantiles) sino también las profesionales, las artísticas e intelectuales (explotación o comercialización de derechos de autor o de creaciones industriales), las científicas o las deportivas[49].

Respecto a la segunda nota (la finalidad concurrencial), la norma la presume cuando, por las circunstancias en que se realice, el acto se revele objetivamente idóneo para promover o asegurar la difusión en el mercado de las prestaciones propias o de un tercero[50]. Es lógico que esta finalidad concurrencial se presuma en el caso de las prácticas comerciales, cuya conceptualización exige que estén directamente relacionadas con la promoción, la venta o el suministro de un producto, entendido este como bien o servicio[51]. Aunque la LCD no incluya expresamente una definición de práctica comercial, dado que la incorporación de esta noción se produce en transposición de la DPCD, a efectos de esta Ley se deriva *a)* que toda alusión al concepto por parte de la LCD debe entenderse en el sentido de la definición aportada por la DPCD y *b)* que el concepto de acto de competencia desleal integra el concepto de práctica comercial, puesto que sería ilógico que una norma nacional no integre en su ámbito material el supuesto de hecho de la Directiva de la UE de la que es transposición.

La tercera característica (que el acto sea realizado antes, durante o después de una operación comercial o contrato, independientemente de que este llegue a celebrarse o no) se incluyó con el objeto de adaptar la LCD al ámbito de aplicación del art. 3 de la DPCD, ya que la misma se aplica a las prácticas comerciales realizadas «antes, durante y después de una transacción comercial en relación con un producto»[52].

Identificado el ámbito material de ambas normas, es razonable afirmar que las prácticas comerciales basadas en perfiles se incluyen en el ámbito de aplicación de la normativa de competencia desleal, siempre que estén relacionadas (de forma directa o indirecta) con la contratación de un producto o servicio. En cuanto al enjuiciamiento de la deslealtad de la conducta, el análisis de cada práctica basada en la elaboración de perfiles que exploten vulnerabilidades del destinatario deberá reali-

---

[48] SAP de Cantabria de 9 de noviembre de 1994.

[49] Massaguer Fuentes, J. «Ámbito de aplicación de la Directiva», *op. cit.,* pp. 17-32.

[50] Art 1 (2) LCD.

[51] Art. d) DPCD.

[52] El tercer apartado del art. 2 LCD fue así incorporado por el art. 1.2 de la Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores y usuarios.

zarse caso por caso, si bien es posible identificar una serie de indicadores de deslealtad que expondremos en subsiguientes apartados.

2.2. *Especial referencia a la exclusión de determinados destinatarios*

Si bien las prácticas comerciales basadas en perfiles son comprendidas de forma general en el ámbito de aplicación material de la DPCD y la LCD, cabe cuestionar si la exclusión de destinatarios que presenten determinadas características reveladoras de vulnerabilidades puede considerarse una práctica comercial. En otras palabras, uno de los fundamentos básicos de las prácticas comerciales basadas en perfiles es analizar datos personales con el objeto de seleccionar a los destinatarios que el algoritmo detecta como *mejores* en función de diversas variables. Esta selección de destinatarios, como advierten ciertos autores, implica irremediablemente la exclusión de otros, por lo que mientras que el destinatario seleccionado es objeto de una acción, el destinatario excluido es objeto de una omisión[53]. Este fue el caso revelado por ciertos informes que exponían cómo Facebook permitía a los anunciantes excluir a ciertos grupos (como «negros, hispanos y etnias afines») de determinados anuncios basándose en la etnia[54].

Pese a que el ámbito material de la LCD haga referencia a *actos* de competencia desleal, señalaba la doctrina —previamente a la incorporación de la DPCD en nuestro ordenamiento— que el concepto de acto desleal puede tener un contenido más amplio, pudiendo consistir tanto en un obrar positivo como en una omisión[55]. Esta amplia comprensión se confirma en el propio concepto de práctica desleal integrado en la LCD y definido por la DPCD, el cual incluye «todo acto, *omisión*, conducta o manifestación, o comunicación comercial, incluidas la publicidad y la comercialización»[56].

Así las cosas, aunque el examen de deslealtad deba ser casuístico, la práctica comercial consistente en excluir a ciertos perfiles no puede ni debe excluirse *ab initio* del examen de deslealtad, puesto que las anteriores normas abarcan en términos objetivos las omisiones y conductas, siempre y cuando estén relacionadas funcionalmente con la contratación de un producto.

---

[53] Wachter, S. «Affinity profiling and discrimination…», *op. cit.*
[54] Parris, T. y Angwin, J. «Facebook lets advertisers exclude…», *op. cit.*
[55] Massaguer Fuentes, J. «Ámbito de aplicación de la Directiva», *op. cit.,* pp. 17-32.
[56] Art. 2 *d)* DPCD, énfasis añadido.

2.3. *La publicidad basada en perfiles que no guarde relación (directa ni indirecta) con la contratación de productos y servicios*

Abogan ciertos autores por que la actual noción de práctica comercial se acomode a la realidad técnico-sociológica y a los problemas de discriminación que puede entrañar la publicidad basada en perfiles[57]. Ahora bien, bajo la actual conceptualización de las prácticas comerciales, ciertos tipos de anuncios que pueden ser considerados problemáticos en términos sociales pueden no quedar acogidos por la caracterización funcional del concepto, que exige una conexión entre la práctica en cuestión y la promoción, venta o suministro de un producto. Esta necesaria conexión se justifica en el ámbito de aplicación de la norma, que excluye, entre otras, aquellas normas dirigidas a proteger intereses que no son de naturaleza económica, como las disposiciones nacionales sobre la protección de la dignidad humana, la prevención de la discriminación sexual, racial y religiosa, o la representación de desnudos, violencia y comportamiento antisocial[58][59].

Si bien la lista negra de prácticas comerciales desleales incorpora conductas que presentan escasa relación directa con la promoción de productos (como la falsa afirmación de pertenecer a un código de conducta), en dichas prácticas se puede apreciar, aunque sea de forma indirecta, una conexión con la contratación de productos y servicios de una empresa al afectar a la imagen de la misma[60].

Ahora bien, en el entorno digital podemos encontrarnos ante prácticas que no estén ligadas (de forma directa ni indirecta) a la contratación de bienes o servicios y cuya personalización puede dar lugar a resultados discriminatorios. Este sería el caso, por ejemplo, de la exclusión de ciertos destinatarios de ofertas sobre empleo anunciadas por plataformas en línea. A título de ejemplo, LinkedIn e InfoJobs remiten ofertas de empleo a sus usuarios, pero la segmentación de estas ofertas obedece no solo a los intereses de los usuarios, sino también a los filtros previamente establecidos por el ofertante de empleo[61].

---

[57] Narciso, M. «The Unfair Commercial Practices Directive – Fit for Digital Challenges?», *Journal of European Consumer and Market Law*, 4, 2024, pp. 147-150.

[58] Señala así el art. 1 de la DPCD que «(L)a presente Directiva tiene por objeto contribuir al buen funcionamiento del mercado interior y alcanzar un elevado nivel de protección de los consumidores mediante la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre las prácticas comerciales desleales que perjudican a los intereses económicos de los consumidores» (énfasis añadido).

[59] Comisión Europea, *Guía sobre la interpretación…, op. cit.,* p. 7.

[60] Stuyck, J. «The Court of Justice and the Unfair Commercial Practices Directive», *Common Market Law Review*, 3, 2015, pp. 721-752.

[61] Mercader Uguina, J. R. «Discriminación algorítmica y derecho granular: nuevos retos para la igualdad en la era del *big data*», *Labos: Revista de Derecho del Trabajo y Protección*

De esta forma (como sucedió con el caso de los anuncios de empleo gestionados por Facebook) es posible que la selección algorítmica de perfiles se base en parámetros discriminatorios[62].

Si este fuera el caso de anuncios sobre alojamiento, éstos se incluirían en el ámbito de aplicación material de la DPCD y la LCD, ya que se dirigen a promocionar la contratación de un producto. En cambio, los anuncios sobre ofertas de empleo no entrarían en el ámbito material funcional de la DPCD ni la LCD, puesto que no hay una relación directa ni indirecta con la contratación de los productos o servicios de la empresa que oferta el empleo, ni siquiera con promocionar su imagen.

Así las cosas, la única vía normativa para paliar este tipo de anuncios sería la prohibición de la DSA de emitir publicidad basada en perfiles utilizando datos sensibles[63]. En caso de que la selección algorítmica de perfiles no se base en datos sensibles, ni la DSA ni la normativa de competencia desleal serían aptas para abordar este tipo de problemáticas, lo cual no obsta a la aplicabilidad de otro tipo de normas, como puede ser el caso de ciertos preceptos del Reglamento de IA, cuyo posible papel comentaremos en otro lugar.

III. BREVE REFERENCIA AL EXAMEN DE TRES PASOS Y A LA LISTA NEGRA DE PRÁCTICAS DESLEALES HACIA LOS CONSUMIDORES

Una vez constatado que la práctica en cuestión se inserta en el ámbito de aplicación material y personal de la LCD, el siguiente paso será determinar si reúne los caracteres propios de alguna de las prácticas desleales específicamente tipificadas por la norma. A tal fin, tanto la LCD como la DPCD establecen una prueba de tres pasos sólidamente construida en la jurisprudencia del Tribunal de Justicia[64].

Comenzando por una breve referencia a la DPCD, el primer paso para determinar la deslealtad de la práctica sería atender al anexo I de la Directiva, el cual incluye una suerte de lista negra compuesta por todas aquellas prácticas que se presumen desleales en cualquier caso[65]. Si la práctica en cuestión no está incluida en el listado, la Directiva proporciona, como segundo paso, una serie de indicaciones particulares para determinar si se puede calificar la práctica como engañosa

---

Social, vol. 2, núm. 2, 2021, pp. 4-10.

[62] Parris, T. y Angwin, J. «Facebook lets advertisers…», *op. cit.*

[63] Art. 26 (2) DSA.

[64] *Vid. inter alia*, Sentencia del Tribunal de Justicia de la Unión Europea, de 23 de abril de 2009, *VTB-VAB NV contra Total Belgium NV y Galatea BVBA contra Sanoma Magazines Belgium NV*, asuntos acumulados C-261/07 y C-299/07 (ECLI:EU:C:2009:244).

[65] *Vid.* anexo I DPCD.

o agresiva[66]. Por último, en caso de que la práctica en cuestión no se enmarque en ninguna de las disposiciones anteriores, la Directiva ofrece un tercer paso, una cláusula general donde se define de manera amplia el concepto de práctica comercial desleal[67].

Esta prueba de tres pasos se incorporó en la LCD si bien, como advertíamos, concurren ciertas variaciones en torno al ámbito de la Ley y de la Directiva. El primer paso (la lista negra de prácticas comerciales desleales) se regula en el capítulo III de la LCD, dedicado a las prácticas comerciales con los consumidores y usuarios. La LCD incluye así una serie de artículos que regulan prácticas que son desleales con los consumidores en todo caso y en cualquier circunstancia, al igual que el anexo I de la Directiva[68]. El segundo paso, dedicado a disposiciones particulares sobre prácticas engañosas o agresivas, se regula en los arts. 5, 7 y 8 LCD, además de en los artículos 19 y 20 de la LGDCU[69]. Como último y tercer paso, la LCD también incorpora una cláusula general de deslealtad en su art. 4.

En consecuencia, cuando se examine la posible deslealtad de un anuncio basado en perfiles que explote vulnerabilidades del destinatario, el primer paso será determinar si la práctica en cuestión está contemplada en la lista negra. Los supuestos enumerados en esta lista son idénticos en la LCD y en la Directiva, puesto que el texto de esta exigía a los Estados Miembros su inclusión sin introducir modificaciones de ningún tipo. Las modificaciones de los supuestos del listado solo podrán ser introducidas mediante una revisión expresa de la Directiva[70].

En lo que aquí nos atañe, tanto la lista negra de la DPCD como —coherentemente— la lista de la LCD guardan silencio con respecto a la elaboración de perfiles y la explotación de datos personales o vulnerabilidades en sentido genérico. Esto excluye que la práctica sea calificada automáticamente como desleal al tratarse de una lista taxativa. Pero no obsta para que la conducta merezca el reproche de deslealtad bajo el examen de tres pasos. Sucesivamente, el segundo paso consistiría en determinar si la práctica en cuestión presenta los caracteres para constituir una práctica agresiva o engañosa, pudiendo incluso constituir ambas[71].

---

[66] *Vid.* Arts. 6-9 DPCD.

[67] *Vid.* Art. 5 DPCD.

[68] *Vid.* Arts. 19 y 21-31 LCD.

[69] Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (en adelante, LGDCU).

[70] Considerando (17) y art. 5 (5) DPCD.

[71] Un ejemplo sería el caso del *inbox advertising*, es decir, aquella práctica consistente en insertar anuncios bajo la forma de mensajes electrónicos en la bandeja de entrada del usuario, sin que dichos anuncios sean apenas distinguibles del resto de correos electrónicos. A estos efectos, la Sentencia del Tribunal de Justicia de la Unión Europea, de 25 de noviembre

IV. EXAMEN DE DESLEALTAD DE LAS PRÁCTICAS COMERCIALES QUE EXPLOTEN DATOS PERSONALES REVELADORES DE VULNERABILIDAD

1. Encuadre y caracterización como práctica agresiva

La Comisión Europea ha reconocido en la Guía de 2021 sobre la DPCD la necesaria complementariedad entre el RGPD y la DPCD, sobre todo en aquellos casos en los que el comerciante trata ilícitamente datos de los consumidores con fines de elaboración de perfiles. La Guía de la Comisión hace referencia expresa a casos en los que el incumplimiento del RGPD guarda relación con la transparencia de la práctica comercial, al ocultar el propósito comercial de la práctica bajo el uso del adjetivo *gratuito* para describir el servicio digital[72] o al no informar al consumidor de que los datos tratados se utilizarán con fines comerciales[73]. El examen como práctica engañosa de ciertos usos comerciales de datos personales implica que el consumidor hubiera tomado o podido tomar una decisión diferente si hubiera sido informado de forma adecuada sobre estos usos, extremo que no necesariamente se cumple en el caso de la explotación de datos para fomentar diseños adictivos[74].

Por esta razón, ciertas prácticas comerciales basadas en la elaboración de perfiles también pueden dar lugar a preocupaciones que trans-

---

de 2021, StWL Städtische Werke Lauf a.d. Pegnitz GmbH y eprimo GmbH, asunto C-102/20 (ECLI:EU:C:2021:954) declaró que el *inbox advertising* podía constituir una práctica agresiva al realizar proposiciones no solicitadas y persistentes por correo electrónico *(spam).* Los caracteres de la práctica en cuestión situaban a la misma en la lista negra por agresividad (anexo I, punto 26 de la DPCD, cuyo equivalente se encuentra art. 29.2 de la LCD). Sin embargo, consideramos que los caracteres de esta conducta permitían considerarla también como engañosa bajo la modalidad de publicidad encubierta, indicio que también manifestó el Abogado General Jean Richard De La Tour en sus conclusiones (ECLI:EU:C:2021:518). Sin embargo, la inserción del término «anuncio», en la publicidad en cuestión llevó a que los tribunales alemanes (precursores del caso) no llegaran a un acuerdo claro sobre el carácter engañoso de la práctica, dilema que el TJUE consiguió evitar al analizar exclusivamente si la práctica podía ser considerada un caso de *spam.* No han faltado críticas doctrinales al caso, por todas, *vid.* Vivero de Porras, C. «Publicidad ilícita por vía electrónica…», *op. cit.,* Igualmente, la doctrina viene criticando de largo la confección del listado de prácticas desleales *per se*, señalando que hay prácticas engañosas que podrían ser calificadas a su vez como agresivas, por todos, *vid.* Tato Plaza, A. *et al.,* «Actos de engaño y omisiones engañosas», en Tato Plaza, A. Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia…», op. cit.,* pp. 150-152.

[72] Lo que podría incumplir el art. 7 (2) y el punto (22) del anexo I, que prohíben la ocultación del propósito comercial de la práctica.

[73] Lo que supondría una omisión engañosa de información sustancial, conforme al art. 7 (2) y el punto (22) del anexo I, así como un incumplimiento de la exigencia de transparencia y demás requisitos establecidos en los artículos 12, 13 y 14 del RGPD.

[74] Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair commercial practice: the case of hyper-engaging dark patterns», *European Journal of Risk Regulation*, 2024.

cienden el fomento de la transparencia, y que se dirigen al aprovechamiento de vulnerabilidades de los destinatarios gracias a la explotación de datos personales, hayan sido éstos tratados de forma lícita o no. En consecuencia, la Comisión ha comenzado a centrar su atención en lo que denomina «prácticas de persuasión personalizadas […] que pueden resultar manipuladoras y, por tanto, desleales desde el punto de vista del derecho en materia de protección de los consumidores»[75]. Sin embargo, se señala a menudo que la línea entre la persuasión y la manipulación es bastante difusa[76]. La Comisión tampoco contribuye a arrojar luz en torno a un concepto de manipulación, que no es exigido en ningún momento por la normativa como requisito para el reproche de deslealtad.

Así las cosas, sí que es cierto que la Comisión hace uso (a nuestro entender, más acertadamente) de otros conceptos sí exigidos por la DPCD, al advertir que el uso de información sobre vulnerabilidades puede constituir una forma de manipulación en la que el comerciante ejerce una práctica agresiva por *influencia indebida*. De este razonamiento se desprenden dos consecuencias. La primera es que la Comisión tiende a relacionar los conceptos de manipulación e influencia indebida, siendo el segundo (a diferencia del primero) un medio reconocido por la DPCD para influir en la decisión del consumidor sobre una transacción[77]. La segunda consecuencia, resultante de la anterior, es la posible caracterización de la práctica descrita como agresiva.

Esta caracterización se presenta como razonable en aquellos casos en los que el reproche de deslealtad se funde no en la omisión significativa de información, sino en la indebida presión de compra que influye en la conducta del consumidor, en la que se sitúan la mayoría de los supuestos de prácticas agresivas recogidos por la DPCD[78]. De cara a determinar la deslealtad de la práctica en cuestión bajo la modalidad de agresividad, habrá que determinar *a)* si la práctica hace uso del acoso, la coacción o la influencia indebida y *b)* si la práctica merma de forma importante la libertad de elección o conducta del consumidor medio con respecto al producto y, por consiguiente, le hace o puede

---

[75] Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 1-129,

[76] Por todos, Cialdini, R. B. «Harnessing the Science of Persuasion», *Harvard Business Law Review*, 2001, pp.1-10 y De Pelsmacker, P. «How advertising works» in *Advanced Introduction to advertising*, pp. 65-75.

[77] Arts. 8 y 9 DPCD.

[78] Distingue así Massaguer que las prácticas agresivas se pueden clasificar principalmente en dos grupos: los tradicionales supuestos de prácticas molestas (como el spam) y los actos de indebida presión de compra, en los que el fundamento de deslealtad se funda precisamente en la aptitud para influir de forma reprobable en la conducta de mercado de los consumidores, sin que el reproche de deslealtad quede sometido (a diferencia de en el caso de las prácticas molestas) a la invasión inaceptable de la esfera privada. Massaguer Fuentes, J. «Las prácticas comerciales agresivas», en Massaguer Fuentes, J., *El nuevo derecho contra…*, *op. cit.,* pp. 131-138.

hacerle tomar una decisión sobre una transacción que, de otra forma, no hubiera tomado.

2. Medios de agresividad. La relevancia del contexto y las líneas grises entre el acoso y la influencia indebida: ¿es necesaria una diferenciación?

Tanto la DPCD como la LCD exigen el empleo del acoso, la coacción o la influencia indebida para la caracterización de una práctica como agresiva[79]. Apenas un año después de la aprobación de la Directiva, ya advertía la doctrina que las diferencias entre estos supuestos no son fáciles de establecer, como bien evidenciaba el hecho de que en la legislación alemana todos estos supuestos quedasen comprendidos en la categoría de influencia indebida sobre la libertad de decisión de los afectados[80]. Ahora bien, en la actual redacción de la UWG, la norma sí que distingue entre diferentes medios por los que la práctica puede ser agresiva, incluyendo no solo la influencia indebida, sino también el acoso y la coacción. Esta inclusión no es sino fruto de la transposición de la DPCD al ordenamiento alemán[81].

Comenzando por el acoso, ni la DPCD ni la LCD incluyen una conceptualización de este, si bien podría definirse como el hecho de perseguir, importunar, incomodar o apremiar a una persona como medio para obtener su decisión de compra o para determinar su comportamiento en el marco de una relación establecida[82]. Siguiendo esta configuración, el acoso presupone un cierto contacto personal entre el empresario y el destinatario de la conducta[83], contacto que se presume por un gran número de autores cuando la publicidad *online* se basa en perfiles[84]. Para calificar una práctica como acoso, debe concurrir no solo este contacto, sino también una serie de circunstancias adicionales que provoquen que el mismo pueda ser percibido por un destinatario medio (normalmente informado y razonablemente atento y perspicaz) como un acoso susceptible de incidir en su libertad de elección[85].

De esta forma, aunque en la publicidad *online* basada en perfiles concurra el requisito general de un contacto directo o estrecho entre

---

[79] Art. 8 (1) LCD y art. 8 DPCD.

[80] Massaguer Fuentes, J. «Las prácticas comerciales agresivas», *op. cit.,* pp. 131-132.

[81] Sección 4a de la UWG.

[82] Massaguer Fuentes, J. «Las prácticas comerciales agresivas», *op. cit.,* pp. 133-134.

[83] Tato Plaza, A. *et al.,* «Prácticas agresivas», *op. cit.,* pp. 181-182.

[84] Galli, F. «Predictive Personalisation», en Galli, F., *Algorithmic Marketing and EU Law on Unfair Commercial Practices*, Law, Governance and Technology Series, vol. 50, 2022, pp. 81-107.

[85] Tato Plaza, A. «Una primera aproximación al régimen jurídico de las prácticas agresivas en la Directiva sobre prácticas desleales con los consumidores», en *Actas de Derecho Industrial y Derecho de Autor*, tomo 27, 2006-2007, p. 433.

el empresario y el destinatario, dicho contacto debe ser razonablemente percibido por este último como acoso. Si la publicidad basada en perfiles presenta los caracteres de una práctica *molesta*, presentando por ejemplo las características de una comunicación no solicitada y persistente, la misma sería calificada automáticamente como *spam*, práctica prohibida *per se* por la lista negra de prácticas desleales[86]. Sin embargo, la publicidad basada en perfiles también puede configurarse como una práctica agresiva no por ser molesta en sí misma, sino por ejercer una indebida presión de compra. En ciertos casos, puede que la explotación de datos sensibles y vulnerabilidades del usuario sea un medio de acoso, constituyendo una forma de perseguir, importunar, incomodar o apremiar a una persona como medio de obtener su decisión de compra.

Tanto la DPCD como la LCD marcan el contexto como un factor relevante para determinar si concurre el acoso[87]. En este punto, dos ejemplos pueden resultar útiles: la discriminación de precios (basada en aplicar diferentes precios a diferentes grupos de consumidores) y la personalización de precios (por la cual el precio es ajustado conforme a técnicas de rastreo *online* y al análisis comportamental de cada consumidor concreto)[88]. Ninguna de estas prácticas es considerada, *per se*, como una práctica desleal siempre y cuando el consumidor resulte debidamente informado. Ahora bien, aunque concurra el requisito de transparencia debida, es posible que las anteriores prácticas puedan tener la calificación de agresivas atendiendo a las circunstancias del caso concreto.

Para identificar la concurrencia de acoso, tanto la LCD como la DPCD tienen en cuenta el momento y lugar en el que se produce la práctica, así como la explotación de cualquier infortunio o circunstancia específicos lo suficientemente graves como para mermar la capacidad de discernimiento del destinatario, de los que el comerciante tenga conocimiento, para influir en su decisión con respecto al bien o servicio[89]. Esta consideración del contexto guarda así una especial relación con el concepto de vulnerabilidad, provocando que la normativa sea particularmente sensible con respecto a las circunstancias específicas en las que se desarrolla la práctica para calificar a la misma como agresiva[90].

Es reseñable que ciertas sentencias del TJUE apuntan a que la lista de factores que la Directiva indica que hay que considerar para determi-

---

[86] Anexo I, punto 26 de la DPCD, cuyo equivalente se encuentra art. 29.2 de la LCD.

[87] Art. 9 DPCD y art. 8 (2) LCD.

[88] Narciso, M. «The Unfair Commercial…», *op. cit.,* pp. 152-153.

[89] Art 9 DPCD y art. 8 LCD.

[90] Kaprou, E. «Aggressive Commercial Practices 2.0: Is the UCPD Fit for the Digital Age?», *Journal of European Consumer and Market Law*, vol. 12, núm. 2, 2023, pp. 76-78.

nar la agresividad de la práctica no es un *numerus clausus.* En este sentido, en el asunto *Orange Polska* el Alto Tribunal considera un factor no contemplado expresamente por el art. 9 DPCD: la concurrencia de «comportamientos que incomodan al consumidor o turban su reflexión relativa a la decisión comercial que ha de tomar»[91]. El carácter abierto de los factores que se pueden tener en consideración permite afirmar que los tribunales nacionales gozan de un amplio margen para apreciar la generalidad de circunstancias que rodean a la práctica en el examen de agresividad[92], amplitud que debe tener una buena acogida a efectos de fomentar el carácter tecnológicamente neutro de la normativa de competencia desleal.

Aunque la discriminación de precios y la personalización de precios no se consideren desleales *per se*, ambas prácticas pueden resultar prácticas agresivas si se aprovechan de situaciones concretas en las que el destinatario resulte especialmente vulnerable. Algunos autores aportan como ejemplo el aumento de precios como consecuencia de pedir el servicio de un vehículo con conductor (VTC) a altas horas de la noche, con bajo nivel de batería en el móvil y en un área poco segura de la ciudad[93]. Otros autores añaden que bajo los infortunios incluidos en la vulnerabilidad se incluyen no solo supuestos generalmente aceptados, como el duelo o la enfermedad, sino también otros factores como una ruptura o el desempleo[94]. Esta amplitud es matizable bajo la normativa nacional, especialmente considerando que —aunque

---

[91] Sentencia del Tribunal de Justicia de la Unión Europea, de 12 de junio de 2019, *Prezes Urzędu Ochrony Konkurencji i Konsumentów contra Orange Polska S.A.,* asunto C-628/17 (ECLI:EU:C:2019:480). Aunque desde luego esta incomodidad del consumidor debe completarse con otros requisitos (la influencia en su capacidad para la toma de decisiones respecto al producto, llevándole o pudiéndole llevar a tomar una decisión sobre una transacción que de otro modo no hubiera tomado) para que la práctica comercial sea desleal, es reseñable la afinidad entre esta interpretación del TJUE y los amplios precedentes alemanes con respecto a la ilicitud de las «prácticas molestas», que actualmente encuentran presencia normativa en la sección 7 de la UWG, regulador de las denominadas «molestias inaceptables».

[92] Helberger, N. *et al., EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets*, BEUC – The European Consumer Organisation, 2023, versión *online*.

[93] Narciso, M. «The Unfair Commercial…», *op. cit.,* pp. 147-153.

[94] Señalan ciertos autores que la configuración de las prácticas agresivas permite integrar conductas tradicionalmente calificadas por la jurisprudencia alemana como «publicidad molesta», en la que las circunstancias son de gran relevancia, como son la publicidad a los familiares en el lecho de muerte (abarcando los momentos previos a la muerte o inmediatamente posteriores) así como la publicidad en caso de accidente (abarcando la visita inmediata a aquellos involucrados en un accidente con el fin comercializar productos o servicios relacionados con el accidente). Tato Plaza, A. *et al.,* «Prácticas agresivas», *op. cit.,* pp. 181-202.

Conviene destacar, respecto al duelo, que el envío de cartas publicitarias sobre lápidas a familiares del fallecido durante las dos semanas posteriores a la muerte fue calificada por un tribunal alemán como una práctica desleal, contraria a la sección 7 (1) de la UWB, la cual indica que «una práctica comercial que constituya una molestia inaceptable para un participante en el mercado es ilegal. Esto se aplica en particular a la publicidad en los casos en que sea evidente que el participante en el mercado solicitado no desea esta publicidad» (Tribunal Regional Superior (Fráncfort del Meno), 29 de enero de 2009, caso núm. 6 U 90/08). Para una reseña del

la DPCD siga un sistema de armonización máxima—[95] siempre queda (en palabras del profesor MASSAGUER) el portillo de las prácticas comerciales contrarias al decoro o al buen gusto[96].

Volviendo a los diferentes canales jurídicos por los que se puede determinar el carácter agresivo de una práctica, también sería razonable plantear si alguna de estas prácticas puede enmarcarse en los otros medios de agresividad recogidos por la norma. En primer lugar, la aplicación de la coacción tendría una virtualidad muy limitada en el caso de prácticas comerciales basadas en perfiles. Aunque no se dispone de un concepto jurídico vinculante para definirla, la coacción se perfila a partir del uso de la fuerza, tanto física como de otra naturaleza, o de la amenaza con su uso[97]. Se defiende igualmente que la coacción psicológica, en cuanto a su empleo inoportuno o molesto, se englobaría en el concepto de acoso, mientras que cuando la misma resulta del sometimiento al poder del oferente podría encuadrarse en la influencia indebida[98]. Así las cosas, parece que la explotación de vulnerabilidades como práctica agresiva se perfila más en torno al uso del acoso o, en todo caso, a la influencia indebida.

Este último medio (la influencia indebida) parece ser la opción preferida por la Comisión al analizar prácticas comerciales que se valgan de información reveladora de vulnerabilidades[99]. La influencia indebida es el único medio de agresividad que sí ha sido definido expresamente por la normativa, siendo identificada con «la utilización de una posición de poder en relación con el destinatario de la práctica para ejercer presión, incluso sin usar fuerza física ni amenazar con su uso»[100]. Aunque la delimitación entre esta y la coacción no parece muy nítida, la influencia indebida introduce claramente la necesidad de que haya una posición de poder con respecto al destinatario, concurriendo *per se* y de forma efectiva —a diferencia de lo que ocurre en la coacción— una capacidad especial de influencia con base en dicha relación de poder.

---

caso en cuestión, *vid.* Fernández Carballo-Calero, P. «Aggressive Commercial Practices…», *op. cit.,* pp. 259-261.

[95] Esta armonización total o «máxima» que recoge la literalidad de la norma ha sido confirmada por la jurisprudencia del TJUE. Por todas, *vid.* Casos conjuntos C-261 & 299/07, Vtb-Vab, EU:C:2009:244. Sobre el carácter numerus clausus de la lista negra de la DPCD, *vid.* Sentencia del Tribunal de Justicia de la Unión Europea, de 11 de marzo de 2002, *Telekommunikacja Polska SA w Warszawie contra Prezes Urzędu Komunikacji Elektronicznej*, asunto C-522/08 (ECLI:EU:C:2010:135).

[96] Considerando 7 DPCD.

[97] Massaguer Fuentes, J. «Las prácticas comerciales agresivas», *op. cit.,* pp. 131-138.

[98] *Ibid.*

[99] Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 28-29.

[100] Art. 8 (1) LCD y art. 2 *j)* LCD.

Señala la doctrina que el concepto de influencia indebida debe ser objeto de una interpretación flexible, subrayando que la posición de poder no tiene que ser ocupada necesariamente por el anunciante[101]. Esta interpretación da pie a sostener que la influencia indebida puede ser llevada a cabo por el medio publicitario o servicio de intermediación, como es el caso de los servicios publicitarios prestados por Meta, Alphabet y Amazon, que ofrecen los mismos de forma combinada con otros servicios digitales, como las redes sociales o los *marketplaces*. La influencia indebida puede así ganar un protagonismo especial en los servicios digitales, en vista de que lleva advirtiéndose de largo que en la mayoría de los servicios digitales en los que el sujeto de datos acepta el tratamiento de datos personales con fines comerciales concurre una gran desproporción de poder entre el sujeto de datos y el prestador del servicio[102].

Resulta extremadamente complejo ofrecer una conceptualización del poder en el marco de la normativa de competencia desleal. Así lo ha puesto de manifiesto la división de la doctrina internacional. GALLI define el poder (en el contexto de la DPCD) como una «dominación intelectual», defendiendo que en el caso de la publicidad personalizada se debe presumir que concurre una alteración del comportamiento económico del consumidor, sin necesidad de ulteriores comprobaciones[103]. Esta visión se antoja excesivamente paternalista, puesto que supondría presumir que toda práctica comercial personalizada es desleal *per se,* y, desde un punto de vista pragmático, debemos recordar que las propuestas para prohibir la publicidad personalizada o comportamental no tuvieron buena acogida en la política legislativa de la UE por resultar excesivas[104]. Sin olvidar que no toda práctica comercial personalizada tiene por qué entrañar efectos perjudiciales para el destinatario, pudiendo resultar positiva o útil para filtrar el exceso de información presente en los mercados digitales.

Otros autores abogan por una aproximación más económica de la noción de poder, haciendo alusión a factores como la cuota de mercado, las barreras de entrada o la rentabilidad[105]. Esta visión no parece tampoco la más coherente en este contexto, puesto que el objetivo de la DPCD es tutelar los intereses económicos de los consumidores y usuarios, si bien es cierto que el ámbito de la LCD pretende proteger la competencia en interés de todos los que participan en el mercado. Desde la óptica de la DPCD sería más razonable interpretar que la referencia a una posición de poder debe entenderse en consideración de las

---

[101] Tato Plaza, A. *et al.,* «Prácticas agresivas», *op. cit.,* pp. 181-202.

[102] Wang, H. J, *et al.* «Research on the Influence Mechanism of Consumers' Perceived Risk on the Advertising Avoidance Behavior of Online Targeted Advertising», *Front Psychol,* 2022.

[103] Galli, F. «Predictive Personalisation», *op. cit.*

[104] Ebers, M. y Sein, K. «Data-driven Technologies…, *op. cit.,* pp. 16-23.

[105] Laux, J. «The shape of personalization to come», *Verfassungblog*, 2023.

relaciones entre la empresa y el consumidor (o, si se prefiere, en conexión con la relación de poder que ostenta el empresario con respecto al consumidor) en vez de acudir a posibles deficiencias estructurales del mercado[106]. Vista de esta forma, la influencia indebida puede concurrir con independencia de que los datos personales se hayan obtenido o combinado de forma lícita conforme al RGPD, la DMA y demás normativa aplicable, puesto que lo determinante es *a)* que concurra una posición de poder y *b)* que la misma sea utilizada para ejercer presión sobre el destinatario, influyendo en su comportamiento económico.

Pese a todos esos razonamientos, sigue sin resultar clara la delimitación entre los diferentes medios de agresividad, particularmente por lo que respecta a la determinación del acoso o el ejercicio de influencia indebida en la explotación de vulnerabilidades. Discusiones terminológicas aparte, lo cierto es que —desde un punto de vista práctico— esta diferenciación no tiene que ser necesariamente llevada a cabo. Esta interpretación es seguida por un reciente estudio publicado por la Comisión Europea para evaluar la adecuación de la normativa de consumo de la UE para abordar la equidad digital, al señalar que los diferentes medios de agresividad pueden solaparse entre sí en una misma práctica[107].

Una interpretación contextual de la normativa confirma que dicha diferenciación no es imprescindible para probar la agresividad de la práctica. Como defiende KAPROU, los artículos 8 (regulador de las prácticas agresivas) y 9 (regulador de los indicadores de acoso, coacción o influencia indebida) de la DPCD no deben ser leídos aisladamente, sino en conjunto[108]. Sostiene la misma autora que una aproximación más pragmática exigiría comenzar por las circunstancias en las que se desenvuelve la práctica y demás factores indicados por el art. 9 DPCD, y, ya conforme al contexto, podría extraerse que concurren uno o más medios de influencia sin necesidad de diferenciarlos, por lo que solo restaría determinar si concurren los demás elementos del art. 8 DPCD[109].

Esta visión conjunta de los arts. 8 y 9 de la Directiva se ha trasladado también a la LCD y a la Ley de Competencia Desleal Alemana (UWG). En ambas, los legisladores nacionales optaron —a nuestro entender acertadamente— por integrar ambos preceptos en uno

---

[106] Duivenvoorde, B. *The Consumer Benchmarks in the Unfair Commercial Practices Directive*, Springer, 2016, pp. 34-36.

[107] Whittle, M. *et al., Study to support the Fitness Check of EU…, op. cit.,* p. 51.

[108] Kaprou, E. «Aggressive Commercial Practices 2.0», *op. cit.,* pp. 76-84.

[109] Es decir, que la práctica en cuestión haga uso de cualquiera de estos medios y, además, merme de manera significativa la libertad de elección o conducta del consumidor medio con respecto al producto y, por consiguiente, le haga o pueda hacerle tomar una decisión sobre una transacción que de otra forma no hubiera tomado.

solo, si bien ambas leyes contienen otros artículos que sí abordan separadamente las prácticas agresivas *per se*, siguiendo la línea de la Directiva[110]. En conclusión, desde un punto de vista probatorio no resulta necesario que al litigar se aleguen estas distinciones (pudiendo una misma práctica amparar todos estos conceptos), si bien es cierto que las mismas pueden ayudar a revelar el significado del término agresivo[111].

3. La afectación del comportamiento económico

Advertíamos previamente que para que la práctica en cuestión merezca la calificación de agresiva no solo es necesario que concurra acoso, coacción o influencia indebida (no siendo éstos excluyentes entre sí), sino que la DPCD exige, además, que la práctica sea susceptible de mermar significativamente la capacidad de elección del destinatario, haciéndole tomar o pudiéndole hacer tomar una decisión que de otro modo no hubiera adoptado[112]. Por su parte, la LCD exige que la práctica «sea susceptible de mermar de manera significativa […] la libertad de elección o conducta del destinatario en relación al bien o al servicio y, por consiguiente, afecte o pueda afectar a su comportamiento económico»[113]. Ambas normas exigen la concurrencia de tres requisitos para que la práctica sea agresiva, todos ellos relacionados con el comportamiento económico del consumidor medio[114]:

1) La práctica debe mermar o poder mermar «de forma importante» la libertad de elección o conducta con respecto al producto (art. 8 DPCD). La formulación que emplea el art. 8.1 de la LCD es casi idéntica, al señalar que la práctica debe ser susceptible de mermar «de manera significativa» la libertad de elección o la conducta con relación al bien o servicio[115].

2) La práctica debe hacer que el consumidor medio tome una decisión sobre una transacción que de otra forma no se hubiera tomado (art. 8 DPCD). La formulación del art. 8.1 de la LCD es notablemente diferente, al hacer referencia a que la práctica debe afectar o poder afectar «el comportamiento económico» del destinatario, si bien esta

---

[110] Respectivamente, art. 8 de la LCD y sección 4a de la UWG.

[111] Fernández Carballo-Calero, P. «Aggressive Commercial Practices…», *op. cit.,* pp. 255-261.

[112] Art. 8 DPCD.

[113] Art. 8 (1) LCD.

[114] Si bien la formulación de sus respectivos preceptos presenta ciertas diferencias terminológicas.

[115] Recordemos que la DPCD emplea el término producto como sinónimo de bien o servicio, por lo que la formulación de ambos preceptos, a efectos funcionales, debe ser entendida como equivalente (art. 2 *c)* DPCD).

divergencia, como expondremos más adelante, no es incompatible con la literalidad de la Directiva.

3) El examen de la totalidad de los requisitos debe ser realizado tomando como referencia al consumidor medio (art. 8 DPCD). Pese a que el art. 8.1 de la LCD hace referencia única al destinatario, el art. 4.2 de la misma Ley aclara que para valorar conductas cuyos destinatarios sean consumidores se tomará como referencia al consumidor medio.

Pasaremos a continuación a exponer cada uno de los siguientes requisitos, distinguiendo casos en los que la explotación de datos reveladores de vulnerabilidades puede afectar al diseño de anuncios concretos o incluso a la generalidad del diseño de un servicio digital.

3.1. *La merma significativa de la libertad de elección con relación al bien o servicio*

Atendiendo a las circunstancias en las que se desenvuelve la práctica en cuestión y determinada la concurrencia de acoso, coacción y/o influencia indebida, es necesario constatar que esta merme o pueda mermar de manera significativa la libertad de elección del destinatario en relación al bien o servicio. Es reseñable que algunas de las prácticas tipificadas como desleales *per se* pueden no cumplir en circunstancias normales con esta condición, como las visitas a domicilio o el envío de publicidad no deseada[116]. Advierte Massaguer que este extremo no debe suponer carta blanca para que los Estados miembros prescindan de este requisito para el reproche de deslealtad de aquellas prácticas comerciales que se valgan del acoso, la coacción o la influencia indebida, si bien es cierto que siempre queda el portillo de que puedan prohibirlas por ser contrarias al decoro o al buen gusto[117].

Así las cosas, la doctrina señala que el requisito de una merma significativa en la libertad de elección exige que el acoso, la coacción o la influencia indebida pongan o puedan poner al destinatario en la situación de decidir contratar el bien o servicio o de no ejercer derechos que le corresponden conforme a lo solicitado o sugerido por la empresa que abusa de su poder[118]. Señala también Massaguer (al hilo de lo marcado por la norma) que para determinar tal merma resulta primordial atender a las circunstancias que componen el contexto en el que se desenvuelve la práctica. En el caso de la publicidad personalizada, las circunstancias determinan el potencial persuasivo de la publicidad

[116] Apartados 25) y 26) de la DPCD, recogidos respectivamente en los apartados primero y segundo del art. 29 LCD.

[117] Massaguer Fuentes, J. «Las prácticas comerciales agresivas», *op. cit.,* pp. 131-138.

[118] *Ibid.*

en cuestión y la capacidad para reducir la autonomía del consumidor en el proceso de toma de decisiones[119].

La Comisión Europea, diversas instituciones (como la OECD o BEUC) y la doctrina internacional han comenzado a prestar particular atención a la merma de la capacidad de decisión de los consumidores a través de los denominados *dark patterns* o patrones oscuros[120]. Según la OECD, el principal factor que caracteriza a estas prácticas se define por los perjuicios que sufren los consumidores. Estos perjuicios pueden dividirse en tres grandes categorías: *a)* pérdidas económicas, *b)* perjuicios a la intimidad, y *c)* perjuicios psicológicos y pérdida de tiempo. Advierte el mismo informe que es probable que estos perjuicios sean acumulativos cuando se emplean varios patrones oscuros a la vez y estén interrelacionados (por ejemplo, la pérdida financiera y de privacidad también puede provocar perjuicios psicológicos)[121].

Aunque a nivel doctrinal no existe una definición unánime, podría señalarse que el denominador común de la generalidad de las conceptualizaciones propuestas para los *dark patterns* es la formulación problemática del diseño como fundamento principal del reproche de deslealtad[122]. A nivel normativo, las únicas definiciones expresas se encuentran en el considerando 67 de la DSA y en el considerando 41 de la Directiva sobre contratos de servicios financieros celebrados a distancia (en adelante, DCSF)[123].

Ambas contienen una conceptualización casi idéntica de los *dark patterns* como aquellas prácticas que distorsionan o merman sustancialmente (de forma deliberada o efectiva) la capacidad de los destinatarios del servicio de tomar decisiones autónomas y con conocimiento de causa o de manera informada[124]. La merma de esta capacidad (si

---

[119] Helberger, N. «Profiling and targeting consumers in the Internet of Things; a new challenge for consumer law,», en Schulze, R. y Staudenmayer, D. (eds.), *Digital revolution: challenges for contract law in practice*, Nomos Baden-Baden, 2016, versión *online*.

[120] OECD. *Dark Commercial Patterns*, *OECD Digital Economy Papers*, núm. 336, 2022, p. 4; BEUC. «Dark Patterns and the EU Consumer Law Acquis», *BEUC Position Paper*, 2022, p. 5; Di Porto, F.; Egberts, A. «The Collective Welfare Dimension of Dark Patterns Regulation», *European Law Journal*, 2023, versión *online*.

[121] OECD. *Dark Commercial Patterns…, op. cit.,* p. 4.

[122] Diversos autores señalan que éstos se identifican con aquellos elementos relativos al diseño de la interfaz que permiten engañar o manipular a los usuarios. Kollmer, T.; Eckhardt, A. «Dark Patterns: Conceptualization and Future Research Directions», en *Business & Information Systems Engineering*, vol. 65, 2022, p. 5. Otros definen este término como aquellas interfaces diseñadas para confundir a los usuarios, dificultar que expresen sus preferencias reales o manipular la toma de determinadas acciones, vid Luguri, J. y Strahilevitz, L. J. «Shining a Light on Dark Patterns», *Journal of Legal Analysis*, vol. 13, núm. 1, 2021, pp. 43-44.

[123] Directiva (UE) 2023/2673 del Parlamento Europeo y del Consejo, de 22 de noviembre de 2023, por la que se modifica la Directiva 2011/83/UE en lo relativo a los contratos de servicios financieros celebrados a distancia y se deroga la Directiva 2002/65/CE.

[124] Las diferencias terminológicas apenas son apreciables y desde luego no parecen significativas. El considerando 41 de la DCSF indica así que «Los elementos engañosos (dark patterns) en

bien en la DPCD se acota al ámbito económico) es un requisito imprescindible para el reproche de deslealtad. Ahora bien, la literalidad de ambas normas marca que estas definiciones se acotan exclusivamente al ámbito de aplicación de cada norma, señalando expresamente la DSA que la regulación incluida en la misma sobre los *dark patterns* no afecta a la DPCD (como tendremos ocasión de desarrollar más adelante)[125].

En el contexto concreto de la DPCD no encontramos una definición expresa de los *dark patterns*[126], si bien es cierto que la Comisión (en la guía sobre la DPCD) utiliza este término para referirse a un tipo de estímulo malintencionado generalmente incorporado en las interfaces digitales de diseño, que puede basarse en datos y personalizarse o aplicarse de forma general aprovechando los sesgos heurísticos o conductuales del destinatario, como los efectos por defecto o los sesgos de escasez[127].

Dependiendo de las circunstancias, se ha señalado que los *dark patterns* pueden ser desleales por *a)* infringir la diligencia profesional del comerciante y demás requisitos de la cláusula general; *b)* constituir una práctica engañosa; o *c)* por constituir una práctica agresiva; sin perjuicio de que el mismo patrón oscuro pueda ser considerado desleal bajo todas estas modalidades[128]. En el caso que aquí más nos

---

las interfaces en línea de los comerciantes son prácticas que distorsionan o merman sustancialmente, bien de forma deliberada, bien de forma efectiva, la capacidad de los consumidores destinatarios del servicio financiero de tomar decisiones autónomas e informadas». El considerando 67 señala por su parte que «Las interfaces engañosas de las plataformas en línea son prácticas que distorsionan o merman sustancialmente, de forma deliberada o efectiva, la capacidad de los destinatarios del servicio de tomar decisiones autónomas y con conocimiento de causa». Es necesario advertir (a efectos de evitar confusiones) que la versión original en inglés de este último considerando de la DSA utiliza expresamente el término dark patterns, mientras que en la versión en español se ha optado por la confusa traducción de «interfaces engañosas». Hubiera resultado francamente deseable que la versión española fuese más coherente con precedentes anteriores (como la guía sobre la DPCD de la Comisión Europea), optando por la traducción «patrón oscuro». Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 28-29.

[125] Art. 25 (2) DSA.

[126] No podemos dejar de advertir que una conceptualización del término *dark pattern* en la normativa reguladora de las prácticas comerciales desleales no resulta necesaria (y para evitar la hiperregulación ya existente, tampoco se presenta como deseable), puesto que ya mayoría de *dark patterns* pueden recaer bajo alguno de los clásicos supuestos de deslealtad que ya contempla la norma. En otras palabras, un *dark pattern* es solo un novedoso concepto para referirnos a aquellas prácticas que puedan ser agresivas, engañosas o contrarias a la cláusula general debido al diseño, pero no dejan de referirse a supuestos que ya tienen una consolidada tradición jurídica. Dicho esto, debido al auge de diseños digitales adictivos o de otra manera problemáticos, puede resultar conveniente hacer una referencia especial a aquellos diseños que (bajo el paraguas *dark pattern*) merezcan el reproche de deslealtad.

[127] La Comisión señala que el «efecto por defecto» se refiere a la tendencia de las personas a seguir por inercia con las opciones que se les asignan por defecto, mientras que el «sesgo de escasez» se refiere a la tendencia de las personas a conceder un valor más alto a las cosas que escasean. Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 30-32.

[128] Luguri, J. y Strahilevitz, L. J. «Shining a Light on Dark…», *op. cit.,* pp. 43-44.

atañe (su examen como práctica agresiva), la explotación de datos personales en el diseño puede constituir un medio para mermar de forma importante la capacidad de elección del destinatario. El diseño ampararía en este contexto la apariencia del anuncio, su contenido (como el producto ofertado, el precio y demás condiciones) y las estrategias en torno a su emisión (como el momento y el medio de presentación o su frecuencia).

Poniendo como ejemplo a la publicidad en los videojuegos en línea, la personalización del diseño de cada anuncio puede resultar ampliamente eficaz para mermar la libertad de elección del usuario, al explotar las emociones de este durante el juego o incluso identificar patrones que revelen una posible adicción. Bajo ciertas circunstancias, la explotación de los datos personales del jugador podría constituir un medio de acoso o de influencia indebida que afecte de forma significativa a su libertad para la toma de decisiones con respecto al producto ofertado.

Un ejemplo sería la introducción estratégica de anuncios para comprar vidas extra en un momento esencial del juego (justo antes de perder) o en el que los datos biométricos (la frecuencia de los clics, la elevación del tono de voz, la dilatación de las pupilas) revelen un estado de excitación o nerviosismo elevado. Bajo estas circunstancias, parece probable que el análisis de datos personales se configure como un medio de acoso (especialmente cuando los anuncios sean persistentes) o de influencia indebida, llevando al jugador a comprar las vidas extra con el fin de evitar las molestias o perturbaciones que los anuncios le ocasionan o las consecuencias negativas de no avenirse a lo anunciado (que serían, en este caso, perder o no conseguir los objetivos marcados).

Dejando aparte la publicidad como práctica concreta, el diseño adictivo de la generalidad del servicio principal también ha sido advertido como un posible instrumento para mermar la capacidad del consumidor de tomar decisiones libres[129]. La amplia conceptualización de las prácticas comerciales da cabida dentro del ámbito de aplicación de la DPCD al propio diseño de un servicio digital, al ser tal diseño una práctica directamente relacionada con la promoción, la venta o el suministro del servicio, siempre y cuando el servicio en cuestión esté dirigido a los consumidores y usuarios[130].

El carácter adictivo de ciertos servicios digitales se ha puesto así en el punto de mira de la Comisión Europea. Conforme al art. 25.1 DSA, «las plataformas en línea no diseñarán […] sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar deci-

[129] Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair…», *op. cit.*
[130] Kollmer, T.; Eckhardt, A. «Dark Patterns…», *op. cit.*

siones libres e informadas»[131]. Conviene advertir que esta previsión de la DSA se enfrenta a las mismas limitaciones subjetivas que la prohibición del art. 26.3 DSA: solo es aplicable a los prestadores de plataformas en línea. Esta limitación significa que ciertos servicios con un diseño potencialmente adictivo (como los videojuegos en línea) no quedan sujetos a prohibición al no presentar las notas características de una plataforma en línea en el sentido de la DSA.

Ahora bien, esta limitación puede salvarse en vista de que la DSA no obsta la aplicabilidad de la DPCD y las normas nacionales que se hayan usado para transponerla, lo cual se refleja en el art. 25.2 de la DSA, al señalar que la anterior prohibición no se aplicará a las prácticas contempladas en la DPCD o en el RGPD[132]. En otras palabras, cuando un determinado *dark pattern* resulte ilícito conforme a la DPCD y/o al RGPD no operará la prohibición de patrones oscuros del art. 26.1 DSA, sometiéndose la conducta al régimen —entendemos más estricto— de la competencia desleal y de protección de datos. La literalidad de la DSA no se opone a que una misma práctica quede abordada simultáneamente por la normativa de transposición de la DPCD y por el RGPD; pero sí excluye, en cambio, la aplicabilidad del art. 26.1 de la DSA para evitar una suerte de doble (o en su caso, triple) sanción añadida a la misma acción relevante[133].

Independientemente de estas exclusiones, no podemos dejar de advertir que el art. 26.1 de la DSA y la DPCD pueden beneficiarse de una relación sinérgica. Por un lado, la DPCD puede servir para abordar aquellos *dark patterns* empleados por empresas que no tengan la consideración de plataformas en línea, ya que el sujeto activo de la DPCD es mucho más amplio que aquel del art. 26.1 DSA. Por su parte, la DSA puede servir para abordar aquellas prácticas que no queden cubiertas por el reproche de deslealtad de la DPCD, al no afectar estrictamente al comportamiento económico de los destinatarios. La DSA solo exige que el diseño distorsione la capacidad de tomar decisiones libres e informadas, sin necesidad de que la práctica perjudique los intereses económicos de los consumidores[134].

En lo que aquí interesa (el examen de agresividad de los *dark patterns* basados en datos personales), veníamos advirtiendo que los patrones oscuros abarcan no solo prácticas comerciales concretas

---

[131] El posible incumplimiento de esta obligación ya ha llevado a la Comisión Europea a abrir investigaciones contra Facebook, Instagram y TikTok, si bien las investigaciones se centran en posibles efectos adictivos sobre los niños.

[132] Ebers, M. y Sein, K., «Data-driven Technologies…, *op. cit.,* pp. 16-23.

[133] Conclusión que se deriva de la literalidad del art. 25.2 de la DSA, al indicar que la «prohibición del apartado 1 no se aplicará a las prácticas contempladas en la Directiva 2005/29/CE o en el Reglamento (UE) 2016/679».

[134] Trzaskowski, J. «Persuasion, Manipulation…», *op. cit.,* pp. 325-328.

como la publicidad basada en perfiles, sino también el diseño de un servicio digital[135]. En el caso de los diseños adictivos, ciertos autores han comenzado a utilizar el término *hyper-engaging dark patterns* (patrones oscuros de *hiperparticipación*), caracterizados por provocar que el usuario pase más tiempo en el servicio gracias al análisis de *big data* y de ciertos rasgos de comportamiento[136]. Estos patrones presentan una potencialidad especial para mermar la capacidad de decisión del consumidor con respecto a las condiciones en las que usa un servicio o a la frecuencia con la que accede al mismo.

El examen de las circunstancias vuelve a presentarse aquí como esencial. El diseño adictivo y su capacidad para afectar a la libertad de decisión del consumidor deben contemplarse globalmente a través de una miríada de elementos: el *scrolling* o desplazamiento infinito por la pantalla, las reproducciones automáticas, las notificaciones *push*, las ventanas emergentes, el sistema de *likes* o «me gusta», los emojis, el número de visualizaciones de los propios contenidos, las historias que desaparecen después de un corto período de tiempo e incluso los seguidores[137].

El denominador común de todos estos elementos es la conjunta merma de atención en los usuarios, comprometiendo su capacidad de tomar decisiones racionales y provocando que reaccionen de una manera automática y predecible por el sistema de IA o algoritmo empleado, entrenado para realizar predicciones (bastante exactas) sobre el comportamiento futuro del usuario y adaptar los contenidos en consecuencia, de forma que se refuercen patrones previos sumiendo al usuario en una suerte de burbuja informativa o *filter bubble*.

Como adelantábamos, la merma en la libertad de decisión del consumidor con respecto al servicio es particularmente apreciable en el caso de los patrones oscuros de hiperparticipación, que se basan en explotar los datos personales del usuario. La presencia de estos patrones

---

[135] Siguiendo el ejemplo de los videojuegos en línea, conviene señalar que el reproche de deslealtad también podría enfocarse también en el diseño adictivo del juego en su totalidad, al fomentar este diseño el uso compulsivo de un servicio que presenta fines comerciales. Este fin comercial puede apreciarse en la totalidad de los actuales modelos de negocio seguidos por los videojuegos en línea, siendo dichos modelos variados. En líneas generales, se puede distinguir el modelo por suscripción (a cambio de una remuneración económica y sin anuncios), el modelo mixto (en el que se combina la suscripción y la recepción de publicidad), el modelo «free» (sin suscripción, pero con anuncios) y el modelo «freemium» (por el cual el usuario no paga una suscripción, pero se cobra una tarifa para adquirir características o funcionalidades avanzadas). BEUC, *Monetising Play: Regulating In-Game and In-App Premium Currencies*, Brussels: BEUC, 2023; y Sotelo, F. «Candy Crush Saga: El secreto de un modelo de negocio de éxito», *Marketing for eCommerce*, 29 de septiembre de 2015.

[136] Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair…», *op. cit.*

[137] Todo ello es parte de un sofisticado diseño de algoritmos adaptativos, dirigidos a captar y retener la atención de los usuarios en los que incluye una creciente necesidad de obtener aceptación social en las redes. *Ibid.*, p.15.

es colosal en las redes sociales y en los videojuegos *online*, conocidos por integrar el *Hook Model* (Modelo Hook o de Gancho) en su diseño, estimulando la necesidad del cerebro humano de completar el ciclo completo de la dopamina, lo que, con el tiempo, puede hacer que una persona cree un nuevo hábito o adicción, como el uso compulsivo de un servicio digital[138].

Pese a que la explotación de datos personales para personalizar la totalidad del servicio o de sus anuncios puede constituir una clara merma de la libertad de decisión del usuario, esta merma debe completarse con otro requisito: la toma o posible toma de una decisión que de otro modo el destinatario no hubiera tomado. Así, aunque la explotación de datos personales a través de los *dark patterns* pueda contribuir a mermar de forma importante la capacidad de decisión del jugador de un videojuego *online*, o la del usuario de una red social, dicha explotación debe tener como consecuencia la toma (o posible toma) de una decisión sobre una transacción que de otro modo no hubiera adoptado.

3.2. *La toma (o posible toma) de una decisión sobre una transacción que de otro modo no hubiera adoptado*

La DPCD exige no solo que la práctica comercial en cuestión haga uso del acoso, la coacción o la influencia indebida mermando la libertad de decisión del consumidor con respecto al bien o producto. Exige además otro requisito: la práctica debe hacer o poder hacer que el consumidor medio adopte una decisión sobre una transacción que de otra forma no se hubiera tomado[139]. Como advertíamos, la formulación de este requisito bajo el art. 8.2 de la LCD es notablemente diferente, al subrayar que la práctica debe afectar o poder afectar al comportamiento económico del destinatario, que en el caso de las prácticas dirigidas a consumidores debe identificarse con el consumidor medio[140].

Esta diferencia terminológica no contradice el tenor de la Directiva, puesto que el art. 4.2 de la LCD aclara que «se entiende por distorsionar de manera significativa el comportamiento económico del consumidor medio, utilizar una práctica comercial para mermar de manera apreciable su capacidad de adoptar una decisión con pleno conocimiento de causa, haciendo así que tome una decisión sobre su comportamiento económico que de otro modo no hubiera tomado». En otras palabras, al analizar la agresividad de la práctica debe entenderse que la exigencia de una distorsión del comportamiento económico es sinónimo de la

---

[138] *Ibid.*

[139] Art. 8 DPCD.

[140] Aclara así el art. 4 (2) LCD que «Para la valoración de las conductas cuyos destinatarios sean consumidores, se tendrá en cuenta al consumidor medio».

toma (o posible toma) de una decisión sobre una transacción que sin la incidencia de la misma no hubiera sido adoptada.

Respecto al concepto de decisión transaccional, la jurisprudencia del TJUE revela una interpretación convenientemente flexible. En el caso *Trento Sviluppo,* el Alto Tribunal subrayó que el concepto se define de manera amplia, cubriendo «no solo la decisión de adquirir o no un producto, sino también la que presenta un vínculo directo con esta», aportando como ejemplo los actos preparatorios, que incluyen el desplazamiento del consumidor al punto de venta o el hecho de entrar en este[141]. La decisión transaccional cubre así «toda decisión por la que un consumidor opta por comprar o no un producto y resuelve de qué manera y en qué condiciones efectúa la compra».

Trasladando esta interpretación a prácticas problemáticas que hayamos advertido anteriormente, es razonable afirmar que la explotación de datos personales para facilitar el diseño adictivo de un servicio digital es una conducta que puede llevar al consumidor medio a tomar una decisión sobre una transacción, que quizá no hubiese adoptado de no mediar dicho diseño. En este sentido, la decisión transaccional sería el acceso continuado (incluso excesivo) a un servicio digital que, de no ser por su diseño adictivo, no sería utilizado de esta manera por el consumidor. La misma lógica se aplicaría a la práctica comercial consistente en analizar determinados datos personales (como el estado emocional) para determinar en qué momento y bajo qué condiciones se anuncia un determinado producto, como en el caso de la publicidad inserta en ciertos videojuegos *online*.

Un argumento análogo puede aplicarse a la personalización de precios en situaciones en las que el consumidor se encuentra particularmente vulnerable. El análisis de ciertos datos personales reveladores de vulnerabilidad puede determinar la elevación de precios en algunos servicios, como la solicitud de transporte a través de aplicaciones como Uber o Cabify. En otras circunstancias, es posible que el consumidor no aceptase un precio tan elevado, por lo que la explotación de datos personales podría llevar en estos casos al consumidor a tomar una decisión transaccional que de otro modo no hubiera tomado.

Si bien el examen debe ser casuístico, la lista de ejemplos en los que la explotación de datos personales puede llevar al consumidor a tomar este tipo de decisiones determinadas por la concurrencia de la práctica desleal es cada vez más elevada en los mercados digitales. A estos efectos debe subrayarse que el reproche de deslealtad por agresividad debe considerarse utilizando como referencia al consumidor

[141] Caso C-281/12, *Trento Sviluppo SRL,Centrale Adriatica Soc. Coop. Arl v. Autorit. Garante della Concorrenza e del Mercato*, [2013] ECLI:EU:C:2013:859, para. 36.

medio, concepto que —como indicaremos a continuación— puede plantear ciertas disyuntivas.

4. El consumidor medio como referencia para el examen de deslealtad

La DPCD exige que el examen de las prácticas comerciales agresivas se lleve a cabo tomando como referencia al consumidor medio. Conforme a reiterada jurisprudencia del Tribunal de Justicia de la Unión Europea se trata de un consumidor «normalmente informado y razonablemente atento y perspicaz»[142]. Si bien el art. 8.1 de la LCD hace referencia exclusiva al destinatario de prácticas agresivas, en lo que aquí nos atañe debemos entender este concepto como equivalente al del consumidor medio, ya que el art. 4.2 de la Ley aclara que «para valorar conductas cuyos destinatarios sean consumidores se tomará como referencia al consumidor medio». Aunque el art. 4 LCD regule la denominada cláusula o prohibición general de deslealtad, y las prácticas agresivas se apliquen con autonomía respecto a esta, la interpretación de las prácticas agresivas debe ajustarse a las exigencias sistemáticas que emanan de la prohibición general en relación con la caracterización del juicio de deslealtad[143].

Así las cosas, todos los factores que componen las prácticas agresivas deben considerarse desde la perspectiva del consumidor medio. En otras palabras, deberá examinarse si la práctica en cuestión merma o puede mermar de forma significativa (mediante el acoso, la coacción o la influencia indebida) la libertad de elección o conducta de un consumidor normalmente informado y razonablemente atento y perspicaz y, por consiguiente, le haga o pueda hacerle adoptar una decisión sobre una transacción que de otra forma no hubiera tomado. La DPCD acoge esta conceptualización con la idea de evitar medidas nacionales que prohíban declaraciones solo susceptibles de engañar a un consumidor sumamente crédulo, ingenuo o superficial (por ejemplo, a través de las exageraciones)[144]. Como defiende la Comisión Europea, esta represión sería desproporcionada y crearía un obstáculo injustificado al comercio[145].

En línea con una interpretación flexible, la referencia al consumidor medio no debe entenderse como una *referencia estadística*, como bien

---

[142] Art. 5 y considerando (18) DPCD. Por todas, Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 1998, *Gut Springenheide GmbH y Rudolf Tusky contra Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung*, asunto C-210/96 (ECLI:EU:C:1998:369), para. 31.

[143] Massaguer Fuentes, J. «Las prácticas comerciales agresivas», *op. cit.,* pp. 131-132.

[144] Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 7-8.

[145] *Ibid.*, pp. 9-10.

aclara el considerando 18 de la DPCD[146], llegándose a afirmar que la noción de consumidor medio no es otra cosa que una *ficción jurídica*[147]. Señala en la misma línea el TJUE que la interpretación del concepto debe ser abierta, en vista de que las autoridades y órganos jurisdiccionales nacionales deben ser capaces de determinar si una práctica puede inducir a error al consumidor medio aplicando su propio criterio y teniendo en cuenta las expectativas generales que se presuman de un consumidor medio, sin necesidad de encargar informes periciales ni la realización de sondeos de opinión[148].

Sin embargo, se ha advertido (y no sin cierta razón) que esta caracterización clásica del consumidor medio como razonablemente informado, atento y perspicaz puede ser inadecuada para hacer frente a determinadas prácticas comerciales personalizadas, ya que los consumidores no siempre actúan ni toman decisiones razonablemente[149]. La interpretación jurisprudencial del TJUE sobre el consumidor medio presume que este presenta una cierta actitud crítica hacia las comunicaciones comerciales y que esa actitud le permite tomar decisiones racionales[150]. Sin embargo, dicha conceptualización ignora que todo consumidor puede ser irracional en aquellos casos en los que la personalización comercial permite apelar a sus vulnerabilidades, ya sea de forma global, ya sea en contextos específicos[151].

---

[146] Si bien no podemos ignorar que esta posibilidad (el uso de estadísticas o informes de expertos por parte del juez nacional) es común en el derecho de marcas para asesorar la percepción de un consumidor medio. *Vid.* Dinwoodie, G. B.; Gangjee, D. S. «The Image of the Consumer in European Trademark Law» in Leczykiewicz, D.; Weatherill, S. (eds.), *The Image(s) of the Consumer in EU Law*, Hart Publishing, 2015, p. 34-35.

[147] Laustsen, R. D. «The Average Consumer in Confusion-Based Disputes in European Trademark Law and Similar Fictions» in *The Average Consumer: A Consumer Fiction in European Trademark Law*, Springer, 2020, p. 127.

[148] Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 1998*, Gut Springenheide GmbH y Rudolf Tusky contra Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung,* asunto C-210/96 (ECLI:EU:C:1998:369), apdos. 31, 32, 36 y 37. Véase también las conclusiones del Abogado General Fennelly, presentadas el 14 de septiembre de 1999, en el asunto *Estée Lauder Cosmetics GmbH & Co. OHG contra Lancaster Group GmbH*, asunto C-220/98, apdo. 28.

[149] Incardona, R.; Poncibò, C. «The average consumer, the unfair commercial practices directive, and the cognitive revolution» in *Journal of Consumer Policy*, vol. 30, 2007, p. 21; Franck, J.-U.; Purnhagen, K. «Homo economicus, behavioural sciences, and economic regulation: On the concept of man in internal market regulation and its normative basis» in Mathis, K. (ed.), *Law and Economics in Europe*, Springer, 2014, p.15; Duivenvoorde, B. *The Consumer Benchmarks…, op. cit.,* p. 36.

[150] Sentencia del Tribunal de Justicia de la Unión Europea, de 20 de febrero de 1979, *Rewe-Zentral AG contra Bundesmonopolverwaltung für Branntwein (Cassis de Dijon*), asunto C-120/78 (ECLI:EU:C:1979:42); Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de septiembre de 2000*, Adolf Darbo AG contra Bundesminister für soziale Sicherheit und Generationen,* asunto C-465/98 (ECLI:EU:C:2000:184); Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de junio de 2015, *Teekanne GmbH & Co. KG contra Verbraucherzentrale Bundesverband e.V.*, asunto C-195/14 (ECLI:EU:C:2015:361).

[151] Incardona, R.; Poncibò, C. «The average consumer…», *op. cit.,* p. 21.

Así las cosas, la referencia al consumidor normalmente informado y razonablemente atento y perspicaz puede ser una vía para regular aquellos casos en los que el consumidor medio es expuesto a prácticas personalizadas, pero conserva en cierta medida un nivel razonable de atención y perspicacia. Este podría ser el caso de la discriminación o la personalización de precios, donde la explotación de datos personales que revelen vulnerabilidades puede ser un método de acoso y/o influencia indebida (como se exponía en apartados anteriores).

La adaptación de precios como consecuencia de la detección de ciertos patrones se basa en la revelación de vulnerabilidades que son circunstanciales (como la urgencia derivada de pedir un coche a altas horas de la noche con bajo nivel de batería o la ausencia de alternativas viables en un barrio poco seguro a altas horas de la madrugada). En estos casos, la explotación de datos personales afecta la capacidad de elección de un consumidor que —aunque sea razonablemente informado, atento y perspicaz— acepta un precio que no pagaría en circunstancias diferentes. Recordemos que el examen de agresividad permite —y exige— tener en cuenta las circunstancias en las que se desenvuelve la práctica, lo que integra en cierto modo la explotación de vulnerabilidades circunstanciales de un consumidor razonablemente atento y perspicaz. En otras palabras: las circunstancias en las que se desenvuelve la práctica pueden ser una vía para moderar las características del consumidor medio.

Dicho esto, también debemos advertir que un examen casuístico mostraría situaciones en las que el consumidor de referencia no es —ni de lejos— razonablemente atento ni perspicaz, ya que la práctica en cuestión solo se ve susceptible de afectar significativamente al comportamiento económico de determinados consumidores vulnerables por factores como la adicción a un servicio. En estos casos, no parece operativo afirmar la agresividad de la práctica, teniendo en cuenta que la jurisprudencia exige un mínimo nivel de actitud crítica y atenta por parte del consumidor[152].

Habida cuenta de estas posibles limitaciones, la noción de consumidor medio parece estar inclinándose hacia una posible reformulación menos exigente con los niveles de atención y perspicacia exigibles. El TJUE pareció moderar esta noción ya en 2012 en el caso *Purely Creative*, al sostener que la explotación de los efectos psicológicos, si está diseñada para influir en el comportamiento del consumidor, puede ser interpretada como un medio de influencia indebida, lo que puede determinar la agresividad de la práctica si concurren los demás

[152] Purnhagen, K. «More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?» in *European Journal of Risk Regulation*, vol. 8, núm. 2, 2017, pp. 437-440.

requisitos aplicables[153]. Este caso fue utilizado en su momento por ciertos sectores de la doctrina internacional para defender que el TJUE estaba abandonando en cierto modo la noción clásica del consumidor medio, si bien algunos autores subrayaron que el caso en cuestión se circunscribía a la lista de prácticas agresivas *per se* (la lista negra), en la que no es necesario realizar el examen general de deslealtad[154].

Diferencias doctrinales aparte, la reformulación del consumidor medio se abrió camino de forma evidente tras el caso *Teekanne*, en el que el TJUE relativizó en cierta medida la consideración del consumidor medio como un consumidor razonablemente atento y perspicaz, al admitir que el mismo «puede mostrarse predispuesto a ignorar o malinterpretar información importante sobre el producto»[155].

La necesidad de reformular el concepto clásico de consumidor medio se plasmó en una petición de decisión prejudicial planteada por el Consejo de Estado Italiano el 13 de octubre de 2022 en el asunto *Compass Banca SpA*[156]. En la primera cuestión prejudicial se planteaba si el concepto de consumidor medio de la DPCD —consumidor normalmente informado y razonablemente atento y perspicaz— debe

---

[153] Sentencia del Tribunal de Justicia de la Unión Europea, de 18 de octubre de 2012, *Purely Creative Ltd y otros contra Office of Fair Trading*, asunto C-428/11 (ECLI:EU:C:2012:651). El Tribunal abordó en este caso el concepto de práctica comercial agresiva en relación con la explotación de los efectos psicológicos sobre los consumidores. El TJUE no clasificó directamente la conducta en cuestión como una práctica «agresiva», sino que subrayó que las prácticas engañosas, como las que les hacían creer a los consumidores que habían ganado un premio cuando en realidad debían incurrir en costos para recibirlo, podrían tener un fuerte impacto psicológico sobre el consumidor. Estas técnicas explotan la expectativa de haber ganado un premio, lo que (según el TJUE) ejerce una presión emocional considerable, afectando su juicio racional. El Tribunal señaló que esta explotación de los efectos psicológicos, si está diseñada para influir en el comportamiento del consumidor, puede ser interpretada como una presión indebida, lo que puede determinar el carácter agresivo de la práctica bajo la Directiva 2005/29/CE si se cumplen las condiciones establecidas para esa categoría. En cualquier caso, el Tribunal no realizó un análisis más detallado de la agresividad de la práctica puesto que la misma ya cumplía con los requisitos para ser considerada engañosa y, por ende, desleal.

[154] Stuyck, J. «The Notion of the Empowered and Informed Consumer in Consumer Policy and How to Protect the Vulnerable Under Such a Regime», en *The Yearbook of Consumer Law 2007*, 1.ª ed., Routledge, 2007, pp. 19-20.

[155] En el caso en cuestión, la empresa demandada (*Teekanne*) comercializaba un té de frutas con imágenes de frambuesas y flores de vainilla en el envase, aunque el producto no contenía esos ingredientes. El TJUE falló que dicho etiquetado podría engañar a los consumidores, incluso si la lista de ingredientes era correcta, ya que el empaque en su conjunto no debe crear una impresión falsa sobre la composición del producto Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de junio de 2015, *Teekanne GmbH & Co. KG contra Verbraucherzentrale Bundesverband e.V.*, asunto C-195/14 (ECLI:EU:C:2015:361). Este caso ha sido visto como una abertura para reconocer sesgos cognitivos en el consumidor medio. *Vid.* Hacker, P. «Manipulation by algorithms…», *op. cit.*; y Purnhagen, K. «More Reality in the CJEU's…», *op. cit.,* pp. 437-440.

[156] Petición de decisión prejudicial planteada por el Consiglio di Stato (Italia) el 13 de octubre de 2022 — Compass Banca SpA/Autorità Garante della Concorrenza e del Mercato (Asunto C-646/22).

ser actualizado considerando las teorías contemporáneas de la *racionalidad limitada*. Estas teorías sugieren que, en la práctica, los consumidores toman decisiones que no siempre son racionales en comparación con un consumidor hipotéticamente atento y perspicaz[157]. La pregunta cuestiona si, dada la creciente complejidad de las dinámicas de mercado, se debería otorgar una mayor protección a los consumidores frente a influencias cognitivas que puedan afectarlos en sus decisiones económicas[158].

El Abogado General Emiliou sostuvo en sus conclusiones generales que el consumidor medio no es necesariamente un individuo racional que adopta una actitud proactiva en la obtención de la información pertinente, procesa racionalmente la información que se le facilita y, por tanto, puede tomar decisiones con conocimiento de causa. Defiende que, si bien en determinadas situaciones puede considerarse que el consumidor medio está en condiciones de actuar racionalmente y de tomar una decisión con conocimiento de causa, el concepto es suficientemente flexible para ser percibido, en otras situaciones, como una persona con una racionalidad limitada que actúa sin obtener toda la información pertinente o es incapaz de procesar racionalmente la información que se le facilita, incluida la información que le presenta el comerciante[159].

Estas cuestiones fueron resueltas por el TJUE en una sentencia de noviembre de 2024 que ha sido ampliamente comentada[160]. El Alto Tribunal llega a las siguientes conclusiones: *a)* el concepto de consumidor medio debe ser interpretado, en términos generales, por referencia al paradigma de un consumidor normalmente informado y razonablemente atento y perspicaz que, por tanto, opera con plena racionalidad, si bien *b)* el paradigma general anterior no obsta para que, en determinadas situaciones relevantes y acreditadas, el juez o tribunal le otorgue una especial protección teniendo en cuenta su ra-

---

[157] Bush, C. y Fletcher, A. *Harmful Online Choice Architecture: How Digital Design Can Harm Consumers and Undermine the Consumer Acquis*, CERRE, 2022, p.28.

[158] La literalidad de la primera cuestión prejudicial es la que sigue: «Dada la elasticidad e indeterminación del concepto de "consumidor medio" que se emplea en la Directiva 2005/29/CE, entendido como consumidor normalmente informado y razonablemente atento y perspicaz ¿no sería conveniente quizá formularlo a la luz de las mejores prácticas del sector y, por consiguiente, atendiendo no solo a la noción clásica de homo economicus, sino también a las conclusiones de las más recientes teorías sobre la racionalidad limitada, que han demostrado que las personas actúan a menudo reduciendo la información necesaria y adoptando decisiones "no razonables" en comparación con las que adoptaría una persona supuestamente atenta y perspicaz, y que exigen una mayor protección de los consumidores en el caso —cada vez más habitual en las modernas dinámicas del mercado— de riesgo de condicionamiento cognitivo?».

[159] Conclusiones del abogado general Sr. Nicholas Emiliou presentadas el 25 de abril de 2024. Asunto C-239/23.

[160] Sentencia del Tribunal de Justicia de 14 de noviembre de 2024, asunto C-646/22, *Compass Banca SpA,* ECLI:EU:C:2024:957. Por todos, *vid.* Tapia Hermida, F. J. «El "consumidor medio", los sesgos cognitivos y las prácticas comerciales desleales de venta cruzada de préstamos y seguros», *La Ley Unión Europea*, núm. 131, Sección Sentencias seleccionadas, 2024.

cionalidad limitada por estar afectado «por sesgos cognitivos consistentes en los límites impuestos a su capacidad cognitiva por el número de estímulos recibidos, la capacidad de permanecer atento en el tiempo, la capacidad de conservar en la memoria toda la información recibida, etc.», y *c)* la inducción de un comportamiento racionalmente limitado del consumidor medio a través de la utilización de sesgos cognitivos puede potenciarse gracias al uso de determinados sistemas de inteligencia artificial prohibidos o calificados de alto riesgo por la AIA.

Esta interpretación podría acoger aquellas prácticas comerciales que explotan vulnerabilidades, particularmente adicciones, con el objetivo de llevar a un consumidor concreto a tomar decisiones comerciales que, de otro modo, no hubiera adoptado. Advertíamos esta posibilidad anteriormente, al señalar, de una forma más general, que la relevancia de las circunstancias o el contexto en el que se desenvuelve la práctica puede ser una vía para moderar las características exigibles al consumidor medio. Asimismo, la tercera conclusión exige tener en consideración el uso de sistemas de IA prohibidos o de alto riesgo, que tendremos ocasión de analizar más adelante.

Como reflexión final, la interpretación a la que llega el TJUE sobre los sesgos cognitivos ha de considerarse con cautela y moderación. Presenta el riesgo de ser percibida como paternalista y desproporcionadamente restrictiva de la libertad de empresa, cayendo en el ya advertido dogma de proteger al consumidor ignorante en lugar de al consumidor razonablemente atento y perspicaz[161]. Esta contracara ha sido advertida por el Abogado General Trstenjak en el caso *Mediaprint Zeitungs,* en cuyas conclusiones generales sostuvo que el Tribunal de Justicia ha asumido que el consumidor medio es generalmente consciente de cómo funcionan la publicidad y las promociones de ventas en una economía de mercado libre y que los consumidores actuales son mucho más cautelosos e informados debido a sus experiencias publicitarias, advirtiendo que la protección excesiva de los consumidores frente a la publicidad es un argumento paternalista que ya no resulta convincente[162].

Por el momento —y en vista de visiones tan polarizadas— cabe concluir que la actual noción del consumidor medio es una vía poco clara para hacer frente a prácticas comerciales basadas en perfiles individuales, por lo que conviene estudiar dos posibles alternativas (*de lege lata)* que podrían rebajar el nivel de atención o perspicacia exigible al destinatario de referencia. Ambas se encuadran en la denominada

---

[161] Sobre el dogma del consumidor ignorante, una de las primeras referencias se encuentra en Preston, i. L. «Reasonable consumer or ignorant consumer? How the FTC decides». *Journal of Consumer Affairs*, 1974, pp. 248-270.

[162] Opinión del abogado general Trstenjak en el caso C-540/08, *Mediaprint Zeitungs- und Zeitschriftenverlag*, ECLI:EU:C:2010:161, párrafo 104.

cláusula general, que establece: *a)* la posibilidad de medir la deslealtad desde la perspectiva del miembro medio del grupo concreto al que se dirige la práctica[163] o, *b)* en caso de que la misma se dirija a un público general, pero afecte exclusivamente a un grupo de consumidores especialmente vulnerables, también se contempla la posibilidad de medir la deslealtad de la práctica desde la perspectiva del miembro medio de ese grupo de consumidores vulnerables[164].

V. EXAMEN BAJO LA CLÁUSULA GENERAL DE DESLEALTAD

1. Cuestiones generales sobre la cláusula general

Con el fin de reemplazar las cláusulas generales y los principios jurídicos divergentes de los Estados miembros, la DPCD incorporó una prohibición general que abarca las prácticas comerciales desleales que distorsionan el comportamiento económico de los consumidores y que funciona como una norma de cierre del sistema[165]. Como tendremos ocasión de exponer a lo largo del presente apartado, este objetivo no se ha visto enteramente satisfecho en la Ley de Competencia Desleal española, cuya cláusula general permite dudar de la plena adecuación de la norma a la Directiva.

La cláusula general de la Directiva se estructura en cinco partes, si bien su contenido se detalla estrictamente en los tres primeros apartados, conteniendo el tercero ciertas normas especiales relativas a los consumidores vulnerables[166]. El primer apartado establece, sin más

---

[163] Art. 5 (2) *b)* in fine DPCD y art. 4 (1) LCD.

[164] Art. 5 (3) DPCD y art. 4 (3) LCD.

[165] Conforme al considerando 13 de la DPCD, «A fin de conseguir los objetivos comunitarios mediante la eliminación de los obstáculos al mercado interior, es preciso reemplazar las cláusulas generales y principios jurídicos divergentes de los Estados miembros. La prohibición general común establecida por la presente Directiva abarca por ello las prácticas comerciales desleales que distorsionan el comportamiento económico de los consumidores».

[166] La literalidad del art. 5 DPCD reza como sigue:

«1. Se prohibirán las prácticas comerciales desleales.

2. Una práctica comercial será desleal si:

a) es contraria a los requisitos de la diligencia profesional, y

b) distorsiona o puede distorsionar de manera sustancial, con respecto al producto de que se trate, el comportamiento económico del consumidor medio al que afecta o al que se dirige la práctica, o del miembro medio del grupo, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores.

3. Las prácticas comerciales que puedan distorsionar de manera sustancial, en un sentido que el comerciante pueda prever razonablemente, el comportamiento económico únicamente de un grupo claramente identificable de consumidores especialmente vulnerables a dichas prácticas o al producto al que se refieran, por padecer estos últimos una dolencia física o un trastorno mental o por su edad o su credulidad, deberán evaluarse desde la perspectiva del miembro medio de ese grupo. Ello se entenderá sin perjuicio de la práctica publicitaria habitual y legítima

precisiones, una prohibición de las prácticas comerciales desleales[167]. El segundo apartado establece las dos condiciones cumulativas para que una práctica comercial sea desleal, esto es *a)* que sea contraria a los requisitos de la diligencia profesional y *b)* que distorsione o pueda distorsionar de manera sustancial, con respecto al producto de que se trate, el comportamiento económico del consumidor medio al que afecta o al que se dirige la práctica, o del miembro medio del grupo, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores. Este segundo requisito es exigible igualmente en el caso de las prácticas agresivas y engañosas (si bien las mismas no exigen que el empresario contravenga la diligencia debida)[168], con la excepción, eso sí, de las prácticas agresivas y engañosas reguladas en el anexo I, que se reputan desleales *per se.*

El tercer apartado contiene una previsión especial para aquellos casos en los que, entre los consumidores cuyo comportamiento económico pueda resultar distorsionado por la práctica comercial enjuiciada, se encuentren consumidores que pertenezcan a un grupo claramente identificable como especialmente vulnerable y así pueda ser razonablemente previsto por el comerciante. La determinación del riesgo de distorsión sustancial del comportamiento económico no debe efectuarse entonces en atención a la reacción del consumidor medio definido, sino en atención a la reacción del miembro medio de ese grupo especialmente vulnerable[169].

Los apartados cuarto y quinto, respectivamente, se remiten a las prácticas engañosas o agresivas (reguladas de forma específica en otros apartados de la Directiva) y a la lista negra de prácticas comerciales

---

de efectuar afirmaciones exageradas o afirmaciones respecto de las cuales no se pretenda una interpretación literal.

4. En particular, serán desleales las prácticas comerciales que:
   a) sean engañosas según lo establecido en los artículos 6 y 7, o
   b) sean agresivas según lo establecido en los artículos 8 y 9.

5. En el anexo I figura una lista de las prácticas comerciales que se considerarán desleales en cualquier circunstancia. La misma lista única se aplicará en todos los Estados miembros y solo podrá modificarse mediante una revisión de la presente Directiva».

[167] Definidas en el art. 2 *d)* DPCD como «todo acto, omisión, conducta o manifestación, o comunicación comercial, incluidas la publicidad y la comercialización, procedente de un comerciante y directamente relacionado con la promoción, la venta o el suministro de un producto a los consumidores».

[168] Como bien aclaró la sentencia del Tribunal de Justicia de la Unión Europea, de 19 de septiembre de 2013, *CHS Tour Services GmbH contra Team4 Travel GmbH*, asunto C-435/11 (ECLI:EU:C:2013:574). El Tribunal de Justicia dictaminó que si una práctica comercial cumple todos los criterios establecidos en el art. 6 (1) para ser calificada de práctica engañosa en relación con el consumidor, no es necesario determinar si dicha práctica es también contraria a las exigencias de la diligencia profesional contempladas en el art. 5 (2) *a)*, para que pueda considerarse legítimamente desleal y, por tanto, prohibida de conformidad con el art. 5 (1). Esta misma lógica es trasladable, a nuestro entender a las prácticas comerciales que cumplan con los criterios para ser calificadas como prácticas agresivas hacia los consumidores.

[169] Massaguer Fuentes, J. «La prohibición general de las prácticas comerciales desleales», en Massaguer Fuentes, J. *El nuevo derecho contra…*, *op. cit.,* pp. 57-58.

desleales *per se*. La totalidad de la cláusula general refleja el denominado examen o prueba de tres pasos que ha sido desarrollado por la jurisprudencia del TJUE y que hemos expuesto en detalle en otro lugar.

Respecto al ámbito operativo de la cláusula general, esta se aplica a las prácticas comerciales desleales que se produzcan fuera de cualesquiera relaciones contractuales existentes entre un comerciante y un consumidor o tras la celebración de un contrato y durante su ejecución[170]. Esta formulación implica que la cláusula general se aplica con independencia de que llegue o no a perfeccionarse el contrato, al igual que el resto de los preceptos relativos a las prácticas comerciales desleales. La configuración de la cláusula general como ilícito de riesgo o peligro se traslada en que la mera aptitud para distorsionar el comportamiento económico del destinatario de referencia es suficiente para declarar la deslealtad de la práctica, sin que se exija en modo alguno una distorsión efectiva de aquel comportamiento[171].

Para que la práctica en cuestión sea calificada como desleal conforme a la cláusula general, no es suficiente la sola infracción de los requisitos de diligencia profesional, como tampoco lo es por sí misma la distorsión sustancial del comportamiento de los consumidores. De ello se deriva la plena legitimidad de aquellas prácticas que no solo influyen, sino que incluso motivan el comportamiento económico de los consumidores cuando son conformes a los requisitos de la diligencia profesional[172].

Antes de proceder a analizar y comparar los requisitos de la cláusula general bajo la DPCD y la LCD, debe advertirse que esta no debe utilizarse para abordar aquellos actos de competencia desleal que encuentren una tipificación expresa bajo la denominada lista negra o bajo los preceptos generales de prácticas agresivas o prácticas engañosas. Es decir, no debe recurrirse a la cláusula general para justificar un doble juicio de deslealtad de una conducta que cuenta con una tipificación específica. La función de la cláusula general como norma de cierre permite su aplicación solo a aquellas prácticas no tipificadas expresamente, impidiendo —contrario sensu— su aplicación a prácticas o conductas que cuenten con una tipificación expresa[173]. Esta clarificación también ha sido apuntada por el TJUE, cuya jurisprudencia subraya que si una práctica cumple con todos los requisitos para ser engañosa no es necesario que, asimismo, contradiga los requisitos de la diligencia profesional[174].

---

[170] Considerando (13) DPCD.

[171] Tato Plaza, A. *et al.,* «Prácticas agresivas», *op. cit.,* pp. 185-186.

[172] Massaguer Fuentes, J. «La prohibición general de las prácticas…», *op. cit.,* pp. 60-62.

[173] Tato Plaza, A. *et al.,* «Prácticas agresivas», *op. cit.,* pp. 186-187.

[174] Sentencia del Tribunal de Justicia de la Unión Europea, de 19 de septiembre de 2013, *CHS Tour Services GmbH contra Team4 Travel GmbH*, asunto C-435/11 (ECLI:EU:C:2013:574).

En lo que aquí nos atañe, el hecho de que acudamos a la cláusula general se justifica en la falta de una tipificación clara de las prácticas basadas en la explotación de perfiles individuales que revelen vulnerabilidades en el usuario, teniendo en cuenta que la actual noción de consumidor medio parece no acomodarse a ciertas prácticas —como los patrones adictivos— que pueden resultar problemáticas para los consumidores. Debido precisamente a la explotación de sus datos personales, los consumidores no se muestran en estos casos razonablemente atentos ni perspicaces.

Dicho esto, tampoco debemos concluir que deba existir una plena incomunicación entre la cláusula general y los demás preceptos reguladores de prácticas agresivas. Por un lado, dado que el legislador decidió fijar unos presupuestos generales de deslealtad y, por otro, considerando que en la tipificación de los concretos actos de competencia desleal pueden apreciarse principios y criterios valorativos que resultan sumamente útiles para aplicar los conceptos jurídicos indeterminados sobre los que se sustenta la cláusula general, como tendremos ocasión de exponer más adelante[175].

2. El incumplimiento de la diligencia profesional

Comenzando por la cláusula general de la Directiva, el primer requisito para considerar la deslealtad de la práctica en cuestión es que esta sea contraria a los requisitos de la diligencia profesional, definida como «el nivel de competencia y cuidado especiales que cabe razonablemente esperar del comerciante en sus relaciones con los consumidores, acorde con las prácticas honradas del mercado o con el principio general de buena fe en el ámbito de actividad del comerciante»[176]. La norma hace pivotar así la cláusula general sobre dos conceptos jurídicos abiertos e indeterminados, opción que fue recibida positivamente por la doctrina debido a que ambos conceptos eran frecuentemente utilizados en la normativa española y en la de muchos otros Estados[177].

---

[175] Tato Plaza, A. *et al.,* «Prácticas agresivas», *op. cit.,* pp. 181-202. A título de ejemplo, en el caso de la adaptación (marcadamente desestructurada) de la LCD a la DPCD la cláusula general también puede servir para salvar ciertas inconsistencias de determinadas prácticas agresivas. En apartados previos señalábamos que la Directiva exige tomar como referencia al «consumidor medio» para el examen de agresividad, (art. 8 DPCD), mientras que el art. 8 (1) de la LCD hace referencia única al «destinatario». En este caso, la cláusula general sirve para armonizar estas divergencias, al señalar que «para valorar conductas cuyos destinatarios sean consumidores se tomará como referencia al consumidor medio» (art. 4 (2) LCD). Este caso sirve como ejemplificación de que debe existir una lectura conjunta de la LCD o, si se prefiere, una comunicación entre la cláusula general y los demás preceptos.

[176] Art. 2 *h)* DPCD.

[177] Señala el profesor Tato Plaza que el concepto de prácticas honradas se encuentra estrechamente vinculado al de usos honestos que se recoge en el Convenio de la Unión de París, y, por consiguiente, en la normativa de competencia desleal de muchos Estados. Por su parte, el

Entendemos en este sentido que la prohibición general había de valerse de estándares o patrones de conducta genéricos para que su concreción atienda a las circunstancias y condiciones en las que una determinada práctica se desarrolla, circunstancias que advertíamos como esenciales para llevar a cabo el examen de deslealtad en las prácticas agresivas.

La terminología empleada por las distintas versiones lingüísticas de la DPCD revela que nos encontramos ante dos conceptos —la buena fe y las prácticas honradas del mercado— que no son equivalentes, así como tampoco necesariamente cumulativos para determinar si la práctica contradice la diligencia profesional. En otras palabras, una práctica puede ser contraria a la diligencia profesional por incumplir la buena fe y/o las prácticas honestas del mercado, pero para no ser desleal debe cumplir con ambos estándares.

Esta conclusión se deriva de las dispares versiones lingüísticas de la DPCD. La versión española se vale así de la conjunción «o», la alemana de las conjunciones «und/oder», la inglesa de las conjunciones «and/or» y la francesa de las conjunciones «et/ou». Esta terminología, reiteramos, pone de manifiesto que el principio de la buena fe no es en este contexto otra forma de denominar a las prácticas honradas del mercado, sino que nos encontramos ante un estándar de conducta distinto.

Los requisitos de la diligencia profesional a los que deben ajustarse las prácticas comerciales comprenden y, por tanto, exigen en última instancia que las prácticas comerciales sean conformes con dos estándares de conducta diferentes, como son las prácticas honradas del mercado y el principio de la buena fe en el ámbito de la actividad de las empresas (y, en particular, con las exigencias que de ellos se deducen para su configuración en las relaciones de las empresas con los consumidores)[178]. En consecuencia, señalaba en su momento el profesor Massaguer que la Directiva no ofrece a los Estados miembros la posibilidad de escoger un patrón de conducta u otro para integrar los requisitos de la diligencia profesional, sino que ha impuesto la adopción simultánea de uno y otro[179].

En contra de esta aproximación tropieza de una manera evidente la redacción de la cláusula general de la LCD, cuyo art. 4.1 encubre, en realidad, una doble cláusula general. Los dos primeros incisos del apartado primero rezan como sigue:

---

concepto de buena fe ha servido también de base para la formulación de la cláusula general de competencia desleal en legislaciones como la española. Tato Plaza, A. *et al.,* «La nueva cláusula general de represión de la competencia desleal», en Tato Plaza, A. Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia…», op. cit.,* pp. 61-97.

[178] Massaguer Fuentes, J. «La prohibición general de las prácticas…», *op. cit.,* pp. 57-58.

[179] *Ibid.*, pp. 60-61.

> 1. Se reputa desleal todo comportamiento que resulte objetivamente contrario a las exigencias de la buena fe.
>
> En las relaciones con consumidores y usuarios se entenderá contrario a las exigencias de la buena fe el comportamiento de un empresario o profesional contrario a la diligencia profesional, entendida esta como el nivel de competencia y cuidados especiales que cabe esperar de un empresario conforme a las prácticas honestas del mercado, que distorsione o pueda distorsionar de manera significativa el comportamiento económico del consumidor medio o del miembro medio del grupo destinatario de la práctica, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores.

El art. 4.1 de la LCD encubre así una doble cláusula general: la primera (inciso primero) es aplicable a las relaciones entre empresas o consumidores, mientras que la segunda (inciso segundo) es aplicable a las relaciones con consumidores o usuarios[180]. En consecuencia, la aplicación del art. 4.1. requiere una tarea previa: determinar si los destinatarios de la práctica son empresarios o son consumidores.

En el caso de las prácticas comerciales que exploten vulnerabilidades sobre la base de perfiles individuales, la principal preocupación de la normativa es la de proteger a los consumidores y usuarios frente a las explotaciones comerciales de datos personales. Aunque la determinación de los destinatarios depende de múltiples factores (como el tipo de producto anunciado o el medio empleado para su difusión), en la mayoría de los casos problemáticos que hemos expuesto previamente los principales destinatarios suelen ser consumidores y usuarios. Así sucede, por ejemplo, con el uso de patrones oscuros en los videojuegos *online* o con el diseño adictivo de ciertas redes sociales, quedando ambas prácticas insertas en medios dirigidos a individuos que actúan al margen de un interés profesional[181]. Aunque por regla general estos servicios se dirijan a los consumidores, no debemos olvidar que el examen de deslealtad es casuístico y la anterior generalización puede presentar excepciones, como sería el caso de anuncios personalizados que promocionen determinados servicios (como la captación de nuevos clientes) a profesionales del sector a través de LinkedIn (red social dirigida a profesionales).

En el caso de que las circunstancias apunten a que la práctica se dirige hacia los consumidores y usuarios operará el inciso segundo del art. 4 LCD, el cual fue señalado como una *víctima* de la integración fragmentada de la DPCD[182]. El primer presupuesto para que el precep-

---

[180] Tato Plaza, A. *et al.,* «La nueva cláusula general…», *op. cit.,* pp. 63-96.

[181] Si bien la LCD no contiene una definición específica del «consumidor», se entiende que la misma acoge por remisión el art. 2.*a)* de la DPCD, que define al consumidor como «cualquier persona física que, en las prácticas comerciales contempladas por la presente Directiva, actúe con un propósito ajeno a su actividad económica, negocio, oficio o profesión».

[182] Tato Plaza, A. *et al.,* «La nueva cláusula general…», *op. cit.,* pp. 90-93.

to resulte de aplicación (y que refleja ya dicha fragmentación) es la incompatibilidad de la práctica con el principio general de la buena fe objetiva. A diferencia del inciso primero (aplicable con independencia de si los destinatarios son o no consumidores), el inciso segundo precisa que se considerará contrario a la buena fe «el comportamiento de un empresario o profesional contrario a la diligencia profesional, entendida esta como el nivel de competencia y cuidados especiales que cabe esperar de un empresario conforme a las prácticas honestas del mercado».

La diferencia entre esta cláusula y la cláusula general de la Directiva es evidente. Mientras que la Directiva hace pivotar la cláusula general sobre el concepto de diligencia profesional (recurriendo a la buena fe y a las prácticas honestas como fuentes), la LCD (art. 4.1, inciso segundo) hace pivotar la cláusula general sobre el principio de buena fe y para concretar las exigencias de este principio general recurre al concepto de diligencia profesional. El inciso segundo da así a entender que la buena fe se identifica exclusivamente con las prácticas honestas del mercado, ignorando con ello que en la Directiva el principio general de la buena fe se incluyó precisamente para evitar que el juicio de deslealtad se hiciera depender únicamente de las prácticas honestas del mercado. Se permitía así que a través del recurso al principio general de la buena fe se impusiesen normas de conducta distintas de las que se derivan simplemente de aquellas prácticas[183].

Así las cosas, el inciso segundo del art. 4.1 LCD exige como primer requisito que la práctica en cuestión sea contraria a la buena fe, entendiendo que se produce dicho incumplimiento cuando la práctica es contraria a la diligencia profesional. Esta diligencia se entiende como el nivel de competencia y cuidados especiales que cabe esperar de un empresario conforme a las prácticas honestas del mercado. En lo que aquí nos atañe (la explotación de datos personales y vulnerabilidades con fines de publicidad basada en perfiles), ciertos autores han señalado que el tratamiento ilícito de datos comerciales constituiría una práctica que incumple la diligencia profesional, al resultar contraria a las prácticas honestas en el mercado[184]. En caso de que el tratamiento de datos sea efectivamente ilícito, podría apreciarse entonces la deslealtad de la práctica conforme a la cláusula general (sin olvidar, claro

[183] Esta divergencia no es baladí y permite dudar de la plena adecuación del art. 4.1. (inciso segundo) a las exigencias de la Directiva comunitaria que, como señalaba Massaguer, no ofrece a los Estados miembros la posibilidad de escoger un patrón de conducta u otro para integrar los requisitos de la diligencia profesional, sino que ha impuesto la adopción simultánea de uno y otro. Massaguer Fuentes, J. «La prohibición general de las prácticas…», *op. cit.,* pp. 57-98.

[184] Wachter, S. «Affinity profiling and discrimination…», *op. cit.*; y Trzaskowski, J. «Persuasion, Manipulation…», *op. cit.*

está, que debe ser apta para distorsionar de forma efectiva el comportamiento económico del consumidor)[185].

Como se ha destacado a lo largo de este trabajo, se dan ciertos casos problemáticos en los que el tratamiento, la combinación o la explotación de datos con fines de publicidad basada en perfiles no quedan siempre prohibidos a causa de las lagunas ya señaladas en el RGPD, la DMA y la DSA. Sin embargo, estos supuestos sí pueden potencialmente perjudicar de forma significativa el comportamiento económico de los consumidores. Así, se plantea la disyuntiva de si algunas de estas prácticas pueden resultar desleales por contradecir el principio general de la buena fe, al explotar vulnerabilidades del destinatario.

En este sentido, la formulación de la cláusula general de la LCD puede resultar problemática ya que —a diferencia de la DPCD— hace depender la buena fe de las prácticas honestas en el mercado. Si bien el análisis debe ser casuístico, esta aproximación puede llevar a la exclusión de ciertas prácticas que resulten problemáticas no por incumplir los requisitos de transparencia o de licitud de tratamiento, sino por los efectos perjudiciales de dicho tratamiento. A título de ejemplo, la personalización de precios es comúnmente aceptada en el tráfico jurídico con base a la libre fijación de precios[186] y a la libertad de empresa[187], por lo que puede resultar discutible que la personalización de los precios con base a datos personales del destinatario sea una práctica deshonesta en el mercado, especialmente si estos han sido tratados lícitamente y el consumidor es informado adecuadamente de tales usos[188].

Ahora bien, aunque la personalización de precios sea una práctica generalizada, la extensión de su uso no la libera en ninguna medida del reproche de deslealtad que pudiera merecer. Como advierte la doctrina, el juicio de deslealtad en modo alguno puede hacerse depender de su generalización en un concreto sector del mercado[189]. Visto así, queda claro que el examen debe ser casuístico y marcado por las circunstancias que rodean a cada práctica en cuestión.

Siguiendo ejemplos anteriormente expuestos, no parece equiparable que la elevación del precio obedezca a datos que revelen una mayor capacidad económica (como el uso de un teléfono móvil de alta gama)

---

[185] A esta deslealtad se le podría unir incluso la deslealtad por violación de normas, en caso de que concurran los requisitos pertinentes que exponíamos en otro lugar.

[186] Arts. 17.1 LCD y 13 LOCM.

[187] Art. 38 CE.

[188] It is important to highlight, however, that the UCPD does not prohibit price discrimination (i. e., the situation where the trader applies different prices to different groups of consumers) or personalized pricing (i. e., the situation where the trader adjusts the price based on online tracking and on the consumer's behavior), as long as the consumer is adequately informed about it.

[189] Tato Plaza, A. *et al.,* «La nueva cláusula general…», *op. cit.,* pp. 61-97. Massaguer Fuentes, J. «La prohibición general de las prácticas…», *op. cit.,* pp. 63-65.

a que se base en datos reveladores de vulnerabilidad (como la baja batería en el móvil a altas horas de la noche en una zona insegura) o a datos personales que puedan dar lugar a un tratamiento discriminatorio injustificado (como el género). De igual forma, podría argumentarse que la creación o fomento de adicciones en el destinatario a través del diseño (*hiper-engaging dark patterns*) contradice el espíritu de las prácticas honestas en el mercado, si bien desde luego hubiera resultado mucho más conveniente que la LCD optase por integrar el concepto general de buena fe de una forma más acorde con la DPCD.

Conviene recalcar, por otro lado, que para que la práctica sea contraria a la diligencia profesional no es necesario que concurra dolo o culpa en su autor. La cláusula general se articula como un ilícito objetivo, lo que desvincula el juicio de deslealtad de cualquier análisis en torno a la intención o voluntad del autor[190]. Siguiendo con los patrones adictivos, es irrelevante que la intención del prestador del servicio sea crear o fomentar una adicción en el usuario a través del diseño, ya que los únicos extremos relevantes a efectos del art. 4 LCD son: *a)* que la práctica sea contraria a la diligencia profesional y *b)* que esta pueda distorsionar el comportamiento económico del consumidor de referencia.

El examen del incumplimiento de la diligencia profesional requiere, por último, determinar la finalidad misma del precepto. En otras palabras, debemos identificar cuál es el propósito de la norma al integrar la ruptura de la diligencia profesional como fuente de deslealtad. En este punto encontramos otro tropiezo por parte del legislador español al trasponer la DPCD en nuestra normativa. Si bien, como advertíamos, el propósito de la Directiva es la tutela de los intereses económicos de los consumidores, este objetivo manifiesto no fue recogido de forma tan expresa en la LCD, que mantiene su redacción original en el artículo primero, identificando como finalidad de la norma «la protección de la competencia en interés de todos los que participan en el mercado».

Divergencias teóricas aparte, en la práctica se ha asumido que toda conducta que limite la autonomía de decisión del consumidor ha de reputarse contraria al principio de competencia de prestaciones que inspira la LCD[191]. En consecuencia, la aplicación del primer requisito (el incumplimiento de la diligencia profesional) debe examinarse en conjunto con el segundo (la aptitud para distorsionar el comportamiento económico de los consumidores). De igual forma, aunque el bien jurídico protegido bajo la LCD sea la competencia económica, no podemos dejar de advertir que la normativa de competencia desleal

[190] Tato Plaza, A. *et al.,* «La nueva cláusula general…», *op. cit.,* pp. 61-97.
[191] *Ibid.*

también es respetuosa con otros valores y derechos constitucionalmente reconocidos, lo que también puede servir como fundamento para un juicio de deslealtad aun cuando la práctica en cuestión no contradiga abiertamente la protección de la competencia en interés de todos los que participan en el mercado. Siguiendo esta aproximación, tanto la Directiva como la LCD han introducido una previsión especial en la cláusula general para abordar el comportamiento económico de un grupo claramente identificable de consumidores o usuarios especialmente vulnerables[192].

Como tendremos ocasión de analizar, el examen de deslealtad tomará entonces como referencia al miembro medio del grupo de consumidores vulnerables especialmente afectado. Se debe hacer hincapié en que el mero incumplimiento de la diligencia profesional no constituye, *per se*, causa suficiente para el reproche de deslealtad bajo la cláusula general. Este reproche debe completarse con un segundo requisito: la posible distorsión del comportamiento económico del consumidor medio (o, en su caso, del miembro medio del grupo de consumidores especialmente vulnerables).

3. La aptitud para distorsionar de forma significativa el comportamiento económico del consumidor

Antes de adentrarnos en el examen del segundo requisito para que opere la cláusula general, conviene recalcar que en ningún modo la cláusula general de la DPCD exige que se produzca una distorsión efectiva del comportamiento económico. El único requisito (además del incumplimiento de la diligencia profesional) es la mera *aptitud* para distorsionar significativamente dicho comportamiento, que no su distorsión efectiva, lo que significa que nos encontramos ante un ilícito de riesgo o de peligro.

Esta potencial distorsión, además, debe ser significativa. Se entenderá por tal la utilización de una práctica comercial para mermar de manera apreciable la capacidad del consumidor de adoptar una decisión con pleno conocimiento de causa, haciendo así que tome una decisión sobre su comportamiento económico que de otro modo no hubiera tomado[193]. Esta distorsión, por su parte, también es exigida en el caso de las prácticas agresivas, en cuyo análisis exponíamos casos en los que la explotación de datos personales puede dar lugar a una afectación significativa del comportamiento económico. Véanse así, en este sentido, los ejemplos ya analizados de la personalización de precios en situaciones en las que el consumidor se encuentra vulnerable,

[192] Art. 5.3 DPCD y art.4.3 LCD.
[193] Art. 4.1 DPCD y art. 2 *e)* DPCD.

la presentación personalizada de anuncios en videojuegos o el diseño adictivo de servicios tales como las redes sociales.

Sin embargo, una gran diferencia de la cláusula general con respecto al reproche de deslealtad en las prácticas agresivas es la posibilidad de evitar la perspectiva del consumidor medio, acudiendo a otras vías de referencia. Estas alternativas se presentan como deseables en el caso de las prácticas comerciales que exploten vulnerabilidades permanentes, temporales o circunstanciales, ya que el consumidor afectado por dichas prácticas puede no presentar las características propias de un consumidor medio, al no mostrarse razonablemente atento ni perspicaz en base, precisamente, a la explotación de dichas vulnerabilidades.

La cláusula general ofrece así dos alternativas, a saber: *a)* en caso de que la práctica comercial se dirija a un grupo concreto de consumidores, medir la deslealtad de la práctica desde la perspectiva del miembro medio de ese grupo concreto[194], o *b)* en caso de que la práctica se dirija a un público general, pero afecte exclusivamente a un grupo de consumidores especialmente vulnerables, medir la deslealtad de la práctica desde la perspectiva del miembro medio de ese grupo de consumidores vulnerables[195].

4. Prácticas comerciales dirigidas a grupos concretos de consumidores: el parámetro del miembro medio del grupo

El examen de deslealtad bajo la cláusula general (tanto en la DPCD como en la LCD) contiene una previsión especial reguladora de aquellos supuestos en los que la práctica comercial en cuestión se dirige a un grupo concreto de consumidores. En estos casos, la distorsión sustancial del comportamiento económico se evaluará desde la perspectiva del miembro medio de ese grupo[196]. Esto significa que el consumidor de referencia no tendrá que ser necesariamente un consumidor razonablemente informado, atento ni perspicaz, pues no se toma como referencia al concepto clásico de consumidor medio, sino que se acude a un concepto distinto: el miembro medio del grupo concreto al que se dirige la práctica comercial. Así, cuando la práctica comercial se remita a un perfil predeterminado y concreto de consumidores, el consumidor de referencia sería el miembro medio de los consumidores que conforman dicho perfil grupal.

Esta valoración del consumidor medio es enormemente relevante, puesto que el miembro medio de ese grupo concreto podría tener unas características o conocimientos más específicos que un consumidor me-

[194] Art. 5 (2) *b)* in fine DPCD y art. 4 (1) LCD.
[195] Art. 5 (3) DPCD y art. 4 (3) LCD.
[196] Considerando (18) y art. 5 (2) *b)* DPCD y art. 4 (1) LCD.

dio no tendría por qué poseer, lo que incide directamente en la evaluación de los efectos de la práctica comercial. *Contrario sensu*, también se entiende que el miembro medio de ese grupo podría tener unos conocimientos menores que los de un consumidor medio general, lo cual dependerá del perfil de consumidores que es objeto del *targeting*[197].

Sin embargo, esta valoración solo opera si el grupo de consumidores es claramente identificable, de carácter limitado y homogéneo, lo que requiere un alto nivel de transparencia en cuanto a los parámetros utilizados por el algoritmo, además de la selección de un grupo concreto de destinatarios. En otras palabras, este precepto resulta operativo cuando las prácticas comerciales se dirigen a perfiles grupales, pero no resulta aplicable para aquellos casos en los que se basa en perfiles individuales, es decir, dirigiéndose a un consumidor concreto por sus características particulares.

Pasando a una perspectiva casuística, podemos señalar que el precepto excluye la publicidad basada en perfiles individuales (como ciertos tipos de publicidad comportamental), pero sí da cabida, en cambio, a la publicidad basada en perfiles grupales (como la publicidad segmentada y la publicidad por afinidad a grupos predefinidos). De igual forma, el precepto excluye de su supuesto de hecho la personalización de precios, puesto que la misma se basa en el análisis comportamental de cada individuo, pero incluye por regla general la discriminación de precios, siempre que los patrones de discriminación permitan realizar agrupaciones claras[198].

En otras palabras, si la práctica comercial está dirigida a grupos concretos identificables, la distorsión del comportamiento económico se medirá desde la perspectiva del miembro medio de ese grupo[199]. Si, por el contrario, no se puede identificar a un grupo concreto, la evaluación debe centrarse entonces en la referencia general del consumidor medio que, como exponíamos, presenta problemas para adaptarse a casos en los que el consumidor al que se dirige la práctica no es razonablemente atento y perspicaz.

La evidente limitación que supone identificar a un grupo concreto de consumidores para que este precepto resulte de aplicación ya ha sido advertida por diversos sectores de la doctrina, que abogan por una reformulación de los consumidores de referencia en la DPCD[200]. Esta necesidad de reformulación también se aprecia en cierto modo en la

---

[197] A título de ejemplo, en un asunto relativo a una publicidad engañosa de pañales infantiles que aludía en particular a una correlación entre las alergias y los pañales del comerciante, se identificó al consumidor medio como los padres de niños pequeños, que carecen de conocimientos específicos acerca de las alergias. Trzaskowski, J. «Persuasion, Manipulation…», *op. cit.*

[198] Narciso, M. «The Unfair Commercial…», *op. cit.,* pp. 147-153.

[199] Comisión Europea, *Guía sobre la interpretación», op. cit.,* p. 34.

[200] Wachter, S. «Affinity profiling and discrimination…», *op. cit.*

Guía de la Comisión sobre la DPCD, si bien la misma presenta evidentes contradicciones.

Por un lado, la Comisión defiende claramente que cuando no se pueda identificar a un grupo concreto la distorsión del comportamiento económico debe evaluarse tomando como referencia al consumidor medio. Por otro lado, al evaluar lo que denomina «prácticas basadas en datos y patrones oscuros», la Comisión señala la posibilidad de que la práctica se evalúe no en función del grupo destinatario, sino desde la perspectiva de una sola persona cuando la práctica es muy personalizada[201].

Esta aproximación, a nuestro entender, choca con la literalidad de la norma y con otros pronunciamientos de la propia Comisión en el mismo documento, que señalan claramente que debe distinguirse un grupo de referencia. Ahora bien, bajo una interpretación funcional podría llegar a argumentarse (si bien muy de lejos y no muy convincentemente) que el grupo de referencia pueda amparar a un solo consumidor como grupo en sí mismo si la práctica es muy personalizada.

Podría llegar a entenderse que la función de la DPCD es proteger no solo los intereses colectivos de los consumidores (lo que justifica la referencia al consumidor medio y a grupos concretos de consumidores), sino que también acoge la protección de los intereses de cada consumidor específico. Este argumento puede encontrar un cierto respaldo en el caso *UPC Magyarország Kft.,* en el que el TJUE aclaró que la DPCD debe interpretarse en el sentido de que la comunicación de una información errónea, como la controvertida en el litigio principal, por parte de un comerciante a un consumidor debe calificarse de práctica comercial engañosa «aun cuando esa comunicación no haya afectado más que a un único consumidor»[202].

En otras palabras, bajo la interpretación del TJUE, no es necesario que una práctica afecte a más de un consumidor para merecer el reproche de deslealtad. Sin embargo, esta interpretación funcional puede no operar en el caso de nuestra Ley de Competencia Desleal que, como ya advertíamos, mantiene su finalidad general de proteger la competencia en interés de todos los que participan en el mercado[203]. Aunque en apartados anteriores se ha señalado que esta finalidad integra la protección de los consumidores y usuarios (aun cuando no se perjudique

---

[201] La literalidad de la guía señala «el valor de referencia de un consumidor medio o vulnerable puede modularse en función del grupo destinatario y, si la práctica es muy personalizada, incluso formularse desde la perspectiva de una sola persona que haya estado sujeta a la personalización específica» Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 1-129.

[202] Sentencia del Tribunal de Justicia de la Unión Europea, de 26 de abril de 2012, *Nemzeti Fogyasztóvédelmi Hatóság contra Invitel Távközlési Zrt*, asunto C-472/10 (ECLI:EU:C:2012:242).

[203] Art. 1 LCD.

de forma directa o evidente a otros operadores), parece dudoso que una interpretación funcional de la misma ampare casos en los que la práctica comercial afecta exclusivamente al comportamiento económico de un solo consumidor.

Ahora bien, tampoco podemos ignorar que la cumulación de prácticas personalizadas que afecten individualmente a diversos consumidores puede tener también un impacto colectivo[204]. Aunque cada práctica comercial varíe conforme a diferentes variables (los *inputs* y *outputs* del algoritmo), el denominador común o efecto de todas estas prácticas es el mismo: la elevación del precio a partir de datos que revelen vulnerabilidades, la adquisición de productos como consecuencia del análisis de datos comportamentales, la creación o fomento de la adicción a un servicio con base a la explotación de datos de consumo y demás ejemplos anteriormente abordados y que damos ahora por reproducidos.

Así las cosas, puede sostenerse que incluso las prácticas comerciales basadas en perfiles individuales tienen un impacto en los intereses colectivos de los consumidores ya que el comportamiento económico de millones de consumidores se está viendo afectado como consecuencia de la explotación de sus datos personales y vulnerabilidades[205]. Una posible vía para aclarar este inciso sería plantear una cuestión prejudicial ante el TJUE, en la que se instase al Tribunal a aclarar la siguiente cuestión:

> ¿Ampara el concepto de «grupo concreto de consumidores» del art. 5.2.*b)* de la DPCD solo a grupos claramente identificables, o debe entenderse que este concepto acoge también a «consumidores individualmente considerados» cuando la práctica sea muy personalizada o no se pueda señalar claramente a un grupo de referencia?

5. Prácticas comerciales que afecten únicamente a grupos identificables de consumidores vulnerables

Se ha señalado previamente que diversas prácticas comerciales basadas en perfiles individuales son susceptibles de apelar a las vulnerabilidades de cada destinatario en concreto basándose, precisamente, en el análisis de sus datos personales. La vulnerabilidad juega un papel especial en la normativa de prácticas comerciales desleales, provocando que la misma se someta a una regulación específica. Sin embargo, es necesario comenzar planteando si las prácticas que hemos señalado

---

[204] De Torres Perea, J. M. «La patrimonialización de datos ante la contaminación digital. Una perspectiva civil ante un reto a nuestro sistema», *Revista de Derecho Civil*, vol. XII, núm. 1, 2025, pp. 279-329.

[205] European Law Institute, *European Commission's Public Consultation on Digital Fairness…, op. cit.,* pp. 22-24.

como problemáticas a lo largo de apartados anteriores tienen cabida dentro del ámbito de aplicación de este inciso, ya que esta acogida podría solucionar potencialmente las incertidumbres advertidas previamente.

Comenzando por el supuesto de hecho del art. 5.3 de la DPCD, este se aplica «a aquellas prácticas comerciales que puedan distorsionar de manera sustancial, en un sentido que el comerciante pueda prever razonablemente, el comportamiento económico únicamente de un grupo claramente identificable de consumidores especialmente vulnerables a dichas prácticas o al producto al que se refieran, por padecer estos últimos una dolencia física o un trastorno mental o por su edad o su credulidad, deberán evaluarse desde la perspectiva del miembro medio de ese grupo».

Las prácticas comerciales integradas en el supuesto de hecho parecen exigir así la concurrencia de tres requisitos no integrados en el supuesto general o apartado segundo: *a)* que la distorsión sustancial del comportamiento económico sea razonablemente previsible por el comerciante; *b)* que la misma pueda afectar únicamente a un grupo claramente identificable de consumidores especialmente vulnerables a dicha práctica o al producto, debido a una dolencia física, un trastorno mental, su edad o su credulidad. Sólo en caso de que concurran todos estos requisitos se rebajará el examen de deslealtad a la perspectiva del miembro medio de ese grupo de consumidores especialmente vulnerables.

La LCD, por su parte, contiene una previsión similar en su art. 4.3, al señalar que «las prácticas comerciales que, dirigidas a los consumidores o usuarios en general, únicamente sean susceptibles de distorsionar de forma significativa, en un sentido que el empresario o profesional pueda prever razonablemente, el comportamiento económico de un grupo claramente identificable de consumidores o usuarios especialmente vulnerables a tales prácticas o al bien o servicio al que se refieran, por presentar una discapacidad, por tener afectada su capacidad de comprensión o por su edad o su credulidad, se evaluarán desde la perspectiva del miembro medio de ese grupo».

Comparando ambos preceptos, la LCD exige los mismos requisitos que la DPCD, si bien añade de forma expresa el siguiente requisito: la práctica comercial debe dirigirse a los consumidores en general, es decir, el precepto solo es aplicable en el caso de las prácticas comerciales dirigidas a un público general, y no en el caso de prácticas comerciales dirigidas a un grupo de consumidores especialmente vulnerables[206]. Este requisito no se encuentra de forma expresa en la DPCD,

[206] Tato Plaza, A. *et al.,* «La nueva cláusula general…», *op. cit.,* pp. 61-97.

si bien puede desprenderse de la lectura conjunta de los apartados segundo y tercero de su art. 5.

En otras palabras, el art. 5.2 DPCD ya regula el caso de las prácticas dirigidas a grupos concretos de consumidores (sean vulnerables o no), señalando que en tales prácticas el examen de deslealtad se tomará desde la perspectiva del miembro medio de ese grupo concreto. Confirma la doctrina que esta variante de la regla general se aplica en los supuestos en los que los consumidores vulnerables no son propiamente los destinatarios específicos de la práctica comercial, sino consumidores que, junto con otros, se encuentran afectados por ella[207].

De este requisito se desprende que el precepto aquí analizado no se aplicará a las prácticas comerciales basadas en perfiles (ya sean individuales o grupales), ya que el supuesto de hecho exige que la práctica comercial se dirija a los consumidores o usuarios en general. En lo que aquí nos atañe, por tanto, se presenta el inconveniente de que se excluyen así las prácticas dirigidas a grupos concretos (perfiles grupales) o a consumidores específicos (perfiles individuales). Debe advertirse que a este inconveniente se le suman otros tantos.

En primer lugar, tanto la DPCD como la LCD exigen que el comerciante pueda prever razonablemente que la práctica pueda afectar únicamente a este grupo de consumidores especialmente vulnerables, medida que se instaura como reflejo del principio de proporcionalidad. Sin embargo, este es un requisito no exigido bajo el supuesto ordinario de la cláusula general, que se configura como un ilícito objetivo, es decir, independiente de la intencionalidad del autor. Así, la inserción de una cierta previsibilidad puede llevar a que el comerciante alegue la concurrencia de resultados algorítmicos imprevistos o poco previsibles, sobre todo en aquellos casos en los que se utilicen sistemas de *machine learning.*

En segundo lugar, el precepto exige la identificación clara de un grupo de consumidores especialmente vulnerables y que el comportamiento afecte únicamente a estos. Este requisito se enfrenta igualmente al desafío de identificar de forma clara a un grupo de consumidores de referencia, a lo que se suma que la práctica debe ser susceptible de afectar de forma significativa *solo* al comportamiento económico de ese grupo. Gran parte de la doctrina aboga desde hace un tiempo por una reformulación de la norma que prescinda de la necesidad de identificar claramente a un grupo de referencia, defendiendo que la vulnerabilidad no depende de grupos sino de contextos y perspectivas variables[208]. Algunos de estos autores sostienen contundentemente que,

---

[207] Massaguer Fuentes, J. «La prohibición general de las prácticas…», *op. cit.,* pp. 57-98.

[208] European Law Institute, *European Commission's Public Consultation on Digital Fairness…, op. cit.,* pp. 22-24,

en lugar de señalar a determinados grupos de consumidores, la vulnerabilidad digital describe un estado universal de indefensión y susceptibilidad a (la explotación de) los desequilibrios de poder que son el resultado de la creciente automatización del comercio, las relaciones entre consumidores y vendedores basadas en datos y la propia arquitectura de los mercados digitales[209].

Ciertos autores señalan, sin embargo, que la referencia a un grupo de consumidores no debe obstaculizar la protección individual del consumidor que es vulnerable debido a su edad, credulidad o discapacidad. Lo contrario llevaría a la absurda conclusión de que la vulnerabilidad debido a las circunstancias excepcionales tuviera más peso que la vulnerabilidad en sí misma[210].

Dicho esto, un problema evidente que puede plantear este requisito es cómo valorar aquellas prácticas comerciales que son susceptibles de afectar el comportamiento económico de más de un grupo (por ejemplo, grupos vulnerables y no vulnerables).

La Comisión señala en este caso que la evaluación debe tener en cuenta a los consumidores realmente afectados por la práctica, con independencia de si se corresponden o no con los destinatarios que el comerciante había previsto[211]. Es decir, si la práctica en cuestión afecta a más de un grupo de consumidores, el examen debe realizarse separadamente desde la perspectiva del miembro medio de cada uno de estos grupos, si bien en el caso de los grupos vulnerables esta posible afectación debe ser previsible por el comerciante. Conforme a este razonamiento, es posible que la práctica pueda distorsionar de forma importante el comportamiento de un grupo que no había previsto, pero era previsible que se viese afectado (por ejemplo, los menores), pero no afecte a otros a los que se dirigía expresamente (por ejemplo, residentes de una determinada zona). De esta forma, el precepto parece tener como objetivo implícito que el comerciante adopte las medidas necesarias para que la práctica no alcance al grupo de consumidores especialmente vulnerables (por ejemplo, debido a su edad).

En tercer lugar, puede plantearse la duda de si las causas de vulnerabilidad que recoge el precepto conforman una lista cerrada o una lista abierta. Bajo una interpretación literal, podría llegar a parecer que es cerrada, ya que la DPCD hace alusión a «un grupo claramente identificable de consumidores especialmente vulnerables a dichas prácticas o al producto al que se refieran, por padecer estos últimos una dolencia física o un trastorno mental o por su edad o su credulidad». Por su parte, la LCD hace referencia a «un grupo claramente identificable

---

[209] Helberger, N. *et al., EU Consumer Protection 2.0, op. cit.*

[210] Fernández Carballo-Calero, P. «Aggressive Commercial Practices…», *op. cit.*

[211] Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 1-129.

de consumidores o usuarios especialmente vulnerables a tales prácticas o al bien o servicio al que se refieran, por presentar una discapacidad, por tener afectada su capacidad de comprensión o por su edad o su credulidad». De esta forma, la LCD opta por el término «discapacidad», en lugar de «una dolencia física», y opta por la expresión «tener afectada su capacidad de comprensión», en lugar de «un trastorno mental».

Diferencias terminológicas aparte, lo cierto es que las mismas no parecen relevantes bajo una interpretación contextual, que revela el carácter abierto del término vulnerabilidad. Así, el considerando 19 de la DPCD hace alusión a «determinadas características *como* la edad, una dolencia física o un trastorno mental o la credulidad» (énfasis añadido), postura que confirma la Comisión al advertir que la DPCD proporciona una lista no exhaustiva de características que hacen que los consumidores sean especialmente sensibles[212].

En conclusión, no parece que la aplicación de este precepto sea una solución óptima para hacer frente a prácticas comerciales basadas en perfiles que exploten las vulnerabilidades de sus destinatarios, debido a que el supuesto de hecho se acota a las prácticas comerciales dirigidas a un público en general, excluyendo así aquellas que estén basadas en la elaboración de perfiles.

VI. NOTAS FINALES

La DPCD —y su transposición a nuestra LCD— presenta como principal ventaja la formulación abierta de determinados supuestos de hecho (concretamente, las prácticas agresivas y la cláusula general de deslealtad) que permiten acoger un gran número de prácticas comerciales que distorsionen el comportamiento económico de los consumidores y usuarios. Pese a ser muy anterior a la normativa previamente analizada (la DSA, la DMA y el RGPD), la Directiva y la LCD se valen de conceptos mucho más flexibles y tecnológicamente neutros e independientes del concepto de datos personales (como el acoso, la influencia indebida o la diligencia profesional), razón por la cual el presente capítulo comenzaba cuestionando si la normativa de competencia desleal puede ser una vía para paliar lagunas no abordadas por los mencionados Reglamentos comunitarios. La conclusión provisional es igual de casuística que la propia normativa de competencia desleal, ya que el reproche de deslealtad en los casos analizados depende principalmente de las circunstancias que rodean a la práctica en cuestión y de si la misma se basa en perfiles grupales o en perfiles individuales.

---

[212] *Ibid.*; European Commission. *Understanding Consumer Vulnerability in the EU's Key Markets*, 2016.

Dependiendo de las circunstancias, la práctica comercial puede ser calificada como agresiva si la misma emplea cualquiera de los medios previstos por la norma (acoso, coacción y/o influencia indebida) de modo que merme de forma significativa la capacidad de elección del consumidor medio, llevándole a tomar una decisión que de otro modo no hubiera tomado. Aunque las circunstancias puedan servir como factor moderador, la actual noción del consumidor medio puede suponer la exclusión de ciertas prácticas personalizadas (como patrones adictivos) que solo afectan a consumidores caracterizados por no ser razonablemente atentos ni perspicaces precisamente porque la práctica apela a vulnerabilidades concretas.

En caso de que la práctica comercial se base en perfiles grupales, el último paso del examen de deslealtad (la cláusula general) puede presentarse como una vía óptima, al abarcar prácticas como la publicidad segmentada o la discriminación de precios, siempre y cuando dichas prácticas se dirijan a un grupo concreto de consumidores (lo que requiere, por su parte, del uso de sistemas algorítmicos o de IA cuyos procesos sean lo suficientemente transparentes y trazables). En estos casos, la cláusula general presenta como ventaja que evita la noción clásica del consumidor medio, que es el principal inconveniente advertido en el examen de las prácticas agresivas.

Ahora bien, el hecho de que la DPCD sea muy anterior a las demás normas analizadas (esto es, a la DSA, a la DMA y al RGPD) presenta como flaqueza que durante el proceso legislativo no se tuviese en cuenta (ni se pudiese tener en cuenta) lo mucho que avanzaría el nivel de personalización de las prácticas comerciales, gracias a procesos como el análisis de *big data* y el auge de complejos sistemas algorítmicos. Así las cosas, y bajo la actual formulación de la DPCD y la LCD, cuando la práctica se dirija al consumidor de forma individual, sin concurrir un grupo de referencia claramente identificable, el examen debe realizarse desde la perspectiva del consumidor medio, con los interrogantes que esta noción acarrea. Incluso aunque se intentase rebajar el examen a la perspectiva del miembro medio de un grupo de consumidores vulnerables, el supuesto de hecho de los consumidores vulnerables exige que la práctica en cuestión se dirija a un público en general, requisito que no concurre cuando la práctica se basa en la elaboración de perfiles.

En otras palabras, cuando la práctica se base en perfiles individuales (supuesto que más nos preocupa), el examen de tres pasos seguido por la normativa de competencia desleal se equipara a una suerte de uróboros. Recapitulando: aplicando el primer paso del examen de deslealtad, la explotación de perfiles que revelen vulnerabilidades no es una práctica prohibida por la lista negra de prácticas desleales. Bajo el segundo paso (el examen de agresividad) se plantea el inconveniente de que el consumidor de referencia es el consumidor medio,

razonablemente atento y perspicaz. En el caso de ciertas prácticas personalizadas (como los patrones adictivos) el principal problema detectado es que el consumidor tiende a no presentar estas características, si bien parece que, tras el caso *Compass Banca SpA,* las circunstancias del caso pueden permitir tener en cuenta la limitación de dicha racionalidad debido a sesgos cognitivos, aunque el paradigma general siga siendo asumir dicha racionalidad y perspicacia. Como vía para evitar la noción de consumidor medio se podría acudir a la cláusula general de deslealtad (tercer paso), si bien la misma plantea como inconveniente que, cuando no se pueda identificar a un grupo de consumidores de referencia, el examen se realizará entonces desde la perspectiva del consumidor medio (retornando, entonces, al problema anterior).

Las potenciales salidas a este círculo pueden ser tres. La primera —ya iniciada por el caso *Compass Banca SpA*— sería rebajar o reformular en cierto modo la noción clásica del consumidor medio, admitiendo que el mismo puede no ser siempre razonablemente atento ni perspicaz, aun cuando sea razonablemente informado. Esta solución, como advertíamos, debe tomarse con cautela, con objeto de no restringir en exceso la libertad de empresa y no sobreproteger al consumidor.

La segunda solución sería entender que el concepto de «grupo concreto de consumidores» del art. 5.2.*b)* de la DPCD y del art. 4.1 de la LCD acoge no solo a grupos claramente identificables, sino también a consumidores individualmente considerados. Es decir, exigiría considerar al consumidor concreto como un grupo en sí mismo cuando la práctica esté sometida a altos niveles de personalización y no se pueda señalar claramente a un grupo de referencia. Esta última interpretación es la que incorpora la Comisión Europea al analizar las prácticas basadas en datos personales y patrones oscuros, si bien debe advertirse que se ha formulado a través de una Guía, instrumento de derecho blando que, lógicamente, no presenta carácter vinculante.[213] No podemos dejar de advertir que la reformulación del consumidor medio es una opción que debe tomarse con cautela y con especial consideración de las circunstancias, con el objeto de no resultar excesivamente paternalista o desproporcionada en vista de las restricciones que puede suponer para la libertad de empresa.

La tercera vía, que plantearemos a continuación y a la que el TJUE presta singular atención en la sentencia *Compass Banca SpA*, consiste en atender a las innovaciones introducidas por la AIA en aquellos casos en los que la práctica comercial se valga de sistemas de Inteligencia Artificial (IA) para manipular la toma de decisiones del destinatario.

---

[213] Comisión Europea, *Guía sobre la interpretación…, op. cit.,* pp. 50-51.

TERCERA PARTE

PRÁCTICAS COMERCIALES PERSONALIZADAS QUE EXPLOTEN VULNERABILIDADES MEDIANTE SISTEMAS DE IA

CAPÍTULO VI

PRÁCTICAS COMERCIALES MANIPULADORAS, SUBLIMINALES O EXPLOTADORAS DE VULNERABILIDADES MEDIANTE SISTEMAS DE IA

I. ALGUNAS NOCIONES PREVIAS SOBRE LAS PRÁCTICAS COMERCIALES PERSONALIZADAS MEDIANTE SISTEMAS DE IA

1. Justificación del examen: carencias de la prohibición de la DSA y relaciones entre la DPCD y la AIA

Comenzábamos este estudio reflexionando sobre el difícil equilibrio de intereses que debe procurar el legislador de la UE para facilitar el avance tecnológico en la Unión al mismo tiempo que garantice que dicho avance se produzca de forma respetuosa con los derechos y libertades fundamentales. Este complejo dualismo se refleja en el objeto de la AIA, cuyo artículo primero pone de manifiesto su doble finalidad: de un lado, mejorar el funcionamiento del mercado interior y promover la adopción de una IA fiable y centrada en el ser humano; y, de otro, garantizar simultáneamente un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales frente a los efectos perjudiciales de los sistemas de IA[1].

[1] Art. 1 (1) AIA.

En este punto, resulta pertinente cuestionarse si la AIA contempla determinadas prácticas comerciales fundamentadas en la explotación de vulnerabilidades. En caso afirmativo, también es relevante examinar cómo lo hace, dado que tales prácticas no han sido abordadas de manera clara por las normativas previamente analizadas (RGPD, DMA, DSA, DPCD), ya sea por las limitaciones de su ámbito de aplicación material o personal.

Sobre estas limitaciones advierte el *Fitness Check 2024*[2], al señalar que la prohibición del art. 26 DSA «se refiere exclusivamente a la publicidad (y no a otras formas de personalización) y no resulta aplicable a operadores económicos distintos de las plataformas en línea. Asimismo, no abarca otras categorías de datos sensibles que puedan estar relacionadas con la vulnerabilidad de los consumidores, como su situación financiera, el historial de juego o un estado anímico negativo»[3].

Leyendo entre líneas, el informe —al igual que este trabajo en secciones anteriores— se muestra en cierta forma crítico con la prohibición del art. 26.3 de la DSA y aboga por la operatividad complementaria de la DPCD, al sostener que «el uso de datos personales sensibles para la publicidad personalizada no se aborda en absoluto en la Directiva sobre Prácticas Comerciales Desleales (DPCD), pero sí en el Reglamento de Servicios Digitales (DSA) únicamente en lo que respecta a las plataformas. No obstante, la DPCD actúa como una salvaguarda al garantizar que las prácticas comerciales desleales estén prohibidas para todos los tipos de operadores económicos»[4].

En otras palabras, el informe pone de relieve las limitaciones de la prohibición del art. 26.3 DSA, tanto respecto a su ámbito personal, acotado a los servicios de plataforma; como a su ámbito material, que deja de lado prácticas comerciales que no tengan cabida en el concepto de publicidad y que depende excesivamente de la problemática noción de datos sensibles. Como posible respuesta, el *Fitness Check 2024* contempla la aplicación de la DPCD, ya que su ámbito de aplicación es mucho más flexible. Si bien la DPCD, como toda Directiva de la UE, presenta el riesgo de resultar en divergencias en su transposición a las normativas nacionales[5], la aproximación que realiza hacia ciertas prácticas comerciales puede resultar convenientemente más flexible que aquella inserta en la DSA, por los mencionados motivos que identifica el *Fitness Check 2024*.

---

[2] Whittle, M. *et al., Study to support the Fitness Check of EU…, op. cit.,* p. 65.

[3] *Ibid.*, p. 66.

[4] *Ibid.*, p. 66.

[5] Sobre las problemáticas que tuvo la transposición de la DPCD al ordenamiento jurídico español, *vid.* Tato Plaza, A. Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia…, op. cit.*

Ahora bien, advertíamos que la DPCD —y su normativa de transposición— plantea interrogantes tales como la formulación actual del consumidor medio. Tradicionalmente, dicho estándar ha venido exigiendo un mínimo nivel de atención y perspicacia. Aunque este paradigma general se mantenga, tras la STJUE *Compass Banca SpA* sus exigencias parecen reducirse en cierta medida en casos en los que la racionalidad del consumidor medio pueda verse afectada por sesgos cognitivos, flexibilización que podría tener importantes repercusiones en prácticas que caigan bajo el paraguas de los patrones oscuros, al fomentar adicciones al servicio o explotar vulnerabilidades detectadas a través del análisis de datos personales[6].

En el caso *Compass Banca*, el Alto Tribunal advierte que la inducción de un comportamiento racionalmente limitado mediante sesgos cognitivos puede potenciarse gracias al uso de determinados sistemas de IA prohibidos por la AIA[7]. Como sostiene Tapia Hermida, en la medida en que los sesgos cognitivos inducidos en la conducta de un consumidor medio se basen en la utilización de este tipo de sistemas de IA prohibidos, las prácticas comerciales podrán verse afectadas por una prohibición en origen, no calificándose solo como agresivas o desleales[8]. Así las cosas, es posible que una práctica comercial que induzca sesgos cognitivos a través de sistemas de IA merezca no solo el reproche de deslealtad, sino que resulte prohibida originariamente por incluirse dentro del catálogo de prácticas prohibidas de la AIA.

El mismo razonamiento se desprende del propio texto de la AIA, al señalar que las prohibiciones sobre técnicas de IA manipulativas, subliminales y explotadoras de vulnerabilidades complementan lo dispuesto en la DPCD[9]. En un idéntico sentido se pronuncia el proyecto de la Comisión sobre prácticas prohibidas de inteligencia artificial (al que nos referiremos como *Directrices sobre prácticas de IA prohibidas*), al señalar que las antedichas prohibiciones se alinean estrechamente con los objetivos de la DPCD, pues el objetivo de ambas normas es «prevenir de manera proactiva los perjuicios a los consumidores derivados de prácticas comerciales impulsadas por la inteligencia artificial que sean manipuladoras, engañosas o agresivas»[10].

---

[6] Sentencia del Tribunal de Justicia de 14 de noviembre de 2024, asunto C-646/22, *Compass Banca SpA,* ECLI:EU:C:2024:957.

[7] *Ibid.*, conclusiones primera a tercera.

[8] Tapia Hermida, F. J. «El "consumidor medio"…», *op. cit.*

[9] Considerando (29) AIA. Estas técnicas constituyen riesgos reputados como inaceptables por el legislador comunitario, lo que determinó que la aplicabilidad de las prácticas prohibidas se adelantase al 2 de febrero de 2025 (a diferencia de la generalidad del Reglamento, que es aplicable a partir del a partir del 2 de agosto de 2026). *Vid.* Considerando (179) AIA.

[10] European Commission, *Communication to the Commission. Approval of the content of the draft Communication from the Commission – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act),* 2025, p. 47 (en adelante, directrices sobre la AIA).

Ante este panorama, se hace imperativo proceder a un análisis de las prácticas prohibidas que han sido objeto de este trabajo en consideración de las reglas de la AIA. Lógicamente el análisis que se realiza a continuación se circunscribe a aquellos casos en que la práctica comercial en cuestión se lleve a cabo a través de sistemas de IA. Por ello, el primer paso requerirá determinar si la práctica en cuestión se vale de estos sistemas de Inteligencia Artificial en el sentido considerado por la AIA.

2. La noción de sistemas de IA en la AIA

Tanto la doctrina como diversos organismos internacionales han propuesto múltiples definiciones de IA[11]. Por lo que respecta sustantivamente a la AIA, este debate ha sido zanjado (no sin antes pasar por un arduo proceso legislativo), acogiendo la última noción aportada por la OCDE[12], definiendo un sistema de IA como aquel «basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales»[13].

Así las cosas, la definición de un sistema de IA puede deconstruirse en cinco notas características: *a)* debe ser un sistema basado en una máquina, *b)* debe estar diseñado para funcionar con distintos niveles de autonomía, *c) puede* mostrar capacidad de adaptación tras el despliegue, *d)* debe tener capacidad de inferencia, y *e)* sus resultados de salida *pueden* influir en entornos físicos o virtuales.

El uso del término «puede» o «pueden» revela que dos de estas notas características son opcionales, por lo que un sistema de IA seguirá siendo caracterizado como tal y caerá bajo el ámbito de aplicación de la AIA aun en el caso de que no muestre capacidad de adaptación, o aunque sus resultados de salida no influyan en entornos físicos o vir-

---

[11] A título de ejemplo, en 2019 el Grupo de expertos de alto nivel sobre la IA definía estos sistemas como «sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido». Grupo de Expertos de Alto Nivel Sobre la IA, *Directrices éticas para una inteligencia artificial fiable*, Comisión Europea, 2019, p.48.

[12] OECD, «Explanatory memorandum on the updated OECD definition of an AI system», *OECD Artificial Intelligence Papers*, núm. 8, OECD Publishing, 2024, p. 5.

[13] Art. 3 (1) AIA.

tuales, si bien estas funcionalidades son relevantes para determinar si nos encontramos ante una práctica prohibida[14]. La opcionalidad de estos requisitos es confirmada por la versión original (en inglés) de la AIA al emplear el verbo *may,* en lugar de optar, por ejemplo, por el vocablo *must*, que sí ofrece una nota de obligación absoluta.

Las anteriores características opcionales reflejan que la definición de los sistemas de IA en la AIA se configura de una forma abierta y elástica, obedeciendo a la voluntad del legislador de la UE de establecer un concepto que abarque y resista futuras innovaciones conforme al principio de neutralidad tecnológica, anunciado desde 2020 con el Libro Blanco sobre IA[15]. Esta flexibilidad también presenta el riesgo de ser identificada con un exceso de ambigüedad[16].

Aunque no presenten carácter vinculante, las *Directrices sobre la definición de sistemas de IA* pueden ayudar a arrojar algo de luz sobre este concepto[17]. A estas directrices contribuyeron ciertos informes relevantes previos, como el del European Law Institute sobre la definición de sistemas de IA y de prácticas de IA prohibidas en el AIA[18]. Este informe se tendrá en consideración durante el presente estudio, aplicado a las prácticas comerciales que hemos identificado como problemáticas en los capítulos anteriores.

2.1. *El sistema debe estar basado en una máquina*

Comenzando por la primera característica (que el sistema esté basado en una máquina) el Reglamento no define qué se ha de entender por una máquina. Bajo una interpretación contextual de la normativa de la UE, la referencia al término «máquina» resulta en cierto modo desafortunada, ya que se presupone que el sistema cuenta con al menos un componente móvil[19].

---

[14] Barrio Andrés, M. «Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial», en Barrio Andrés, M. (dir.) *El Reglamento de Inteligencia Artificial*, Tirant lo Blanch, 2024.

[15] Comisión Europea, *Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*, 2020.

[16] Rubio Bravo, M.ª P. «Tecnologías de reconocimiento facial en las actuaciones previas al procedimiento administrativo sancionador: a propósito del asunto *Glukhin c. Rusia*», *Revista española de derecho administrativo*, núm. 237, 2024.

[17] European Commission, *Communication to the Commission. Approval of the content of the draft…, op. cit.*

[18] European Law Institute (ELI), *Guidelines on the Application of the Definition of an AI System in the AI Act: ELI Proposal for a Three-Factor Approach*, 2024, en adelante, *Informe del ELI sobre la AIA*.

[19] El art. 3.1.*a)* del Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo (Reglamento de Máquinas) define el término máquina como «un conjunto de elementos o componentes vin-

Se limita a ofrecer una conceptualización circular, al señalar que «el término "basado en una máquina" se refiere al hecho de que los sistemas de IA se ejecutan en máquinas», aclaración que aporta poco o nada a efectos interpretativos[20]. Esta ambigüedad puede salvarse o encontrar su justificación en que tal vez resulta más conveniente —desde un punto de vista de neutralidad tecnológica— no acotar el término en la norma para evitar la exclusión de supuestos no comprendidos actualmente en el estado de la técnica.

Para salvar ciertas inseguridades jurídicas que puedan derivar de esta ambigüedad, las *Directrices sobre la definición de sistemas de IA* pueden resultar de utilidad[21]. La Comisión aclara en las mismas que el concepto de «basado en una máquina» hace referencia a la naturaleza intrínseca de los sistemas de IA, los cuales se desarrollan y operan mediante máquinas. A efectos de su definición jurídica, el término máquina debe interpretarse de manera amplia, comprendiendo tanto los componentes de hardware como los de software que posibilitan el funcionamiento del sistema de IA. El hardware abarca los elementos físicos esenciales, como las unidades de procesamiento, la memoria, los dispositivos de almacenamiento, las redes y las interfaces de entrada y salida. Por su parte, el software incluye el código fuente, los programas, los sistemas operativos y las aplicaciones que gestionan el tratamiento de datos y la ejecución de tareas. Conforme a las directrices, todos los sistemas de IA requieren el uso de máquinas a lo largo de su ciclo de vida, incluyendo fases como el entrenamiento de modelos, el procesamiento de datos, la modelización predictiva y la toma automatizada de decisiones a gran escala.

En otras palabras, el elemento «basado en máquinas» destaca que los sistemas de IA son, en esencia, impulsados por procesos computacionales y operaciones realizadas por dispositivos electrónicos. Asimismo, esta noción da cabida a una amplia gama de sistemas computacionales, incluidos aquellos basados en tecnologías emergentes, como los sistemas de computación cuántica. Estos, a pesar de su funcionamiento diferenciado y el empleo de principios de la mecánica cuántica, constituyen sistemas basados en máquinas. Lo mismo ocurre con determinados sistemas biológicos u orgánicos, siempre que proporcionen capacidad de procesamiento computacional.

Aplicando este razonamiento a los sistemas de IA utilizados para personalizar prácticas comerciales (como la publicidad, los precios,

---

culados entre sí, de los cuales al menos uno es móvil, asociados para una aplicación determinada, provisto o destinado a estar provisto de un sistema de accionamiento distinto de la fuerza humana o animal».

[20] Considerando (12) AIA.

[21] European Commission, *Communication to the Commission. Approval of the content of the draft…*, *op. cit.,* pp. 1-12.

o el diseño adictivo de ciertos servicios), el denominador común radica en que funcionan a través de algoritmos de complejidad variable, cumpliendo con el requisito más básico de los exigidos, es decir, que el sistema esté basado en máquinas, entendido de una manera amplia[22].

2.2. *El sistema debe estar diseñado para funcionar con distintos niveles de autonomía*

La segunda característica requiere que el sistema esté diseñado para funcionar con distintos niveles de autonomía. Si bien la formulación de este término es flexible, se entiende que el sistema debe tener un nivel mínimo de autonomía, por lo que se excluyen aquellos sistemas que sean completamente dependientes de la intervención humana[23]. Así lo aclara el considerando 12 de la AIA, al señalar que los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. Estas capacidades son variables dependiendo del sistema de IA ante el que nos encontremos, presentando los sistemas *deep learning* el mayor nivel de autonomía dentro de las clasificaciones generalmente aplicadas a los sistemas de IA[24].

Como tendremos ocasión de desarrollar más adelante, las *Directrices sobre el concepto de sistemas de IA* adelantan que los conceptos de «autonomía» e «inferencia» están intrínsecamente relacionados. La capacidad de inferencia de un sistema de IA es fundamental para la consecución de su autonomía, ya que esta autonomía depende de su facultad para generar resultados (tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales).

Las mismas directrices también aclaran ciertas inclusiones y exclusiones de sistemas. El requisito de contar con algún grado de autonomía excluye aquellos sistemas que dependan exclusivamente de la intervención manual directa en todas sus operaciones. Esta intervención puede ser directa (por ejemplo, mediante controles manuales) o indirecta (a través de mecanismos automatizados que permiten la supervisión o delegación por parte del ser humano). Por otro lado, las directrices

---

[22] Sousa E Silva, N., «The Artificial Intelligence Act: Critical Overview», *Social Science Research Network* (SSRN), 30 de julio de 2024.

[23] Novelli, C.; Casolari, F.; Hacker, P.; Spedicato, G.; Floridi, L. «Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity», en *Computer Law & Security Review*, vol. 55, 2024, art. núm. 106066, pp. 1-16.

[24] OECD, «Explanatory memorandum on the updated OECD…», *op. cit.*; y Huergo Lora, A. «Una aproximación a los algoritmos…», *op. cit.*

incluyen expresamente a un sistema que, tras recibir datos de entrada manuales, es capaz de generar de forma autónoma un resultado sin que este haya sido explícitamente determinado por el usuario. Este criterio se aplica, igualmente, a sistemas expertos que, tras una delegación de la automatización de procesos, emiten recomendaciones u otros resultados.

Aunque el análisis deberá ser casuístico, la nota de autonomía está presente con carácter general en las prácticas comerciales personalizadas analizadas en este trabajo. En el ámbito de la intermediación publicitaria, estos servicios de intermediación son generalmente gestionados en la actualidad por los mismos proveedores (Amazon, Meta y Alphabet) que operan bajo complejos sistemas de IA altamente autónomos[25]. A título de ejemplo, Google Ads, Amazon Ads y Meta Ads se caracterizan por ofrecer complejas funcionalidades en sus sistemas de IA generativos, que permiten adaptar el contenido y el diseño del anuncio en tiempo real[26]. Lo mismo sucede en el caso de los sistemas de recomendación. El *Informe del ELI sobre la AIA* aplica un examen a diversos sistemas para determinar si son considerados sistemas de IA conforme a la AIA. Entre ellos se identifica a sistemas de recomendación como los utilizados por Amazon o Spotify.

Esta autonomía también es destacable en la inserción —cada vez más habitual— de publicidad o prácticas comerciales en las conversaciones mantenidas con *chatbots.* Esta práctica genera dilemas sobre su falta de transparencia o carácter subliminal, desde la doble perspectiva de la competencia desleal y de la AIA, así como por el diseño adictivo y personalizado de servicios como las redes sociales y los videojuegos *online*[27]. El *Informe del ELI sobre la AIA* incluye a varios chatbots basados en *large language models* (LLMs) entre los ejemplos de sistemas de IA en el sentido de la AIA.

En suma, aunque los requerimientos normativos de la AIA solo exigen unos niveles mínimos de autonomía para calificar un sistema de IA, los sistemas empleados en la actualidad para personalizar prácticas comerciales *online* presentan altos niveles de independencia con respecto al ser humano, lo que fundamenta —aún más— su encuadre dentro de la noción de IA y el sometimiento a su régimen jurídico. A su vez, como señalan las Directrices sobre la definición de sistemas de IA, este alto nivel de autonomía constituye un factor clave para categorizar el sistema como un sistema de IA prohibido o de alto riesgo.

---

[25] Geradin, D. y Katsifis, D., «An EU competition law analysis…», *op. cit.*

[26] Google, «Powered IA solutions», disponible en *https://ads.google.com/intl/es-419_ALL/home/campaigns/ai-powered-ad-solutions/*; Meta «Business Ads Meta advantage», disponible en *https://en-gb.facebook.com/business/ads/meta-advantage*; Amazon «AI image generation», disponible en *https://advertising.amazon.com/blog/ai-image-generation.*

[27] Laux, J. «The shape of personalization…», *op. cit.*

2.3. *La posible capacidad de adaptación tras el despliegue*

La capacidad de adaptación tras el despliegue se refiere a las posibilidades reales de autoaprendizaje que permiten al sistema cambiar mientras está en uso[28]. Esta característica es opcional, por lo que no constituye un requisito imprescindible para que el sistema caiga en el ámbito de aplicación de la AIA. De esta forma, la AIA ampararía tanto a sistemas de personalización de prácticas comerciales que tengan capacidad de autoaprendizaje tras el despliegue como a los que no.

La posible capacidad de adaptación tras el despliegue guarda ciertas similitudes con el nivel mínimo de autonomía exigible al sistema, si bien las *Directrices sobre la definición de sistemas de IA* aclaran que son dos requisitos diferenciados. Mientras que manifestar un nivel mínimo de autonomía es un requisito imprescindible para que el sistema merezca la consideración de IA, la capacidad de adaptación es un requisito optativo.

Esta naturaleza optativa significa que el sistema publicitario utilizado no tiene por qué modificar sus variables o parámetros tras el despliegue. Como aclaran las *Directrices sobre la definición de sistemas de IA*, la capacidad de un sistema para aprender de manera automática, descubrir nuevos patrones o identificar relaciones en los datos que van más allá de aquellos sobre los que fue inicialmente entrenado constituye una característica facultativa y, por tanto, no representa una condición determinante para establecer si dicho sistema califica como un sistema de IA.

Dicho de otra forma, quedarían amparados tanto aquellos sistemas que sigan de manera inmutable las variables establecidas en el momento de despliegue como aquellos que, con base a datos generados tras el despliegue, modifican las variables de selección de los destinatarios para optimizar los resultados. Así las cosas, la AIA ampara tanto sistemas de IA de enorme simpleza (como los filtros de *spam*) como aquellos de gran complejidad (como los sistemas *deep learning*), si bien las normas aplicables a cada uno de estos sistemas serán considerablemente diferentes. Esta capacidad de adaptación puede determinar que conformen riesgos inaceptables, altos riesgos o riesgos mínimos, cada uno de ellos sometido a requisitos normativos diferentes.

2.4. *La capacidad de realizar inferencias para generar outputs*

De todas las características que configuran la noción de IA en el Reglamento, la cuarta es la que desempeña un protagonismo mayor:

[28] Considerando (12) AIA.

la capacidad de inferencia. Si bien la definición de sistemas de IA del art. 3.1 AIA solo hace referencia expresa a la capacidad de generación de resultados de salida, los considerandos de la norma aclaran que la capacidad de inferencia se desdobla en dos aspectos. Por un lado, la capacidad de inferencia se refiere al proceso de obtención de resultados de salida (como predicciones, contenidos, recomendaciones o decisiones), proceso que *puede* influir en entornos físicos y virtuales, como considera expresamente la definición de sistemas de IA del art. 3.1 AIA. Este sería el caso del sistema de recomendación de Google. Por otro lado, la capacidad de inferencia abarca también la capacidad de un sistema para deducir modelos y/o algoritmos a partir de *inputs* (como el uso de Gemini para la generación de código en lenguajes de programación como Python y JavaScript sobre descripciones en lenguaje natural)[29].

De esta forma, parece que el legislador distingue entre dos conceptos: la generación de resultados de salida y la deducción de modelos o algoritmos; si bien ambos conceptos se encuadran dentro de la capacidad de inferencia que distingue a los sistemas de IA de otros sistemas. Esta interpretación del concepto de inferencia es coherente con la definición contenida en el estándar ISO/IEC 22989, que define la inferencia como el «razonamiento mediante el cual se derivan conclusiones a partir de premisas conocidas», añadiendo una nota específica para el ámbito de la IA, que señala «en inteligencia artificial, una premisa puede ser un hecho, una regla, un modelo, una característica o datos en bruto»[30].

A nivel práctico, tanto las *Directrices sobre la definición de sistemas de IA* como el considerando 12 de la AIA distinguen dos categorías de técnicas que permiten la realización de inferencias: las técnicas de aprendizaje automático y las técnicas basadas en lógica y razonamiento.

En la primera categoría, las *Directrices sobre la definición de sistemas de IA* definen los sistemas de aprendizaje automático como aquellos en los que el sistema aprende a partir de los datos para lograr ciertos objetivos, sin necesidad de ser programado explícitamente para cada tarea. Dentro de este grupo, las directrices distinguen varias subcategorías: el aprendizaje supervisado, el aprendizaje autosupervisado, el aprendizaje por refuerzo y el aprendizaje profundo.

El aprendizaje supervisado es aquel en el que el sistema aprende de datos etiquetados, es decir, datos que ya contienen las respuestas co-

---

[29] Google, «Usa la IA para generar código humano», disponible en *https://cloud.google.com/use-cases/ai-code-generation?hl=es*.

[30] ISO/IEC 22989:2022, «Information technology – Artificial intelligence – Artificial intelligence concepts and terminology», 2022.

rrectas. Este tipo de aprendizaje se utiliza en sistemas de detección de correos electrónicos de spam o en diagnósticos médicos basados en imágenes etiquetadas, entre otros. En contraste, el aprendizaje no supervisado trabaja con datos no etiquetados y permite al sistema descubrir patrones o relaciones dentro de esos datos. Ejemplos de esta técnica incluyen sistemas para la detección de anomalías o el descubrimiento de nuevos medicamentos mediante la agrupación de compuestos químicos.

El aprendizaje autosupervisado es una subcategoría del aprendizaje no supervisado, en la que el sistema utiliza los datos no etiquetados para crear sus propias etiquetas u objetivos. En esta categoría se incluyen, por ejemplo, modelos de lenguaje que predicen la siguiente palabra de una oración o sistemas de reconocimiento de imágenes.

El aprendizaje por refuerzo, por otro lado, es un tipo de aprendizaje en el que el sistema aprende de la experiencia mediante un sistema de recompensas y castigos, como los robots que aprenden a manipular objetos o los vehículos autónomos que optimizan sus movimientos.

Finalmente, el aprendizaje profundo (*deep learning*) es un subconjunto del aprendizaje automático que utiliza redes neuronales profundas, lo que permite aprender características de alto nivel a partir de grandes volúmenes de datos. Este enfoque es utilizado en tareas complejas como el reconocimiento facial, la traducción automática y el procesamiento de lenguaje natural.

En la segunda categoría, las *Directrices sobre la definición de sistemas de IA* definen los enfoques basados en lógica y conocimiento como aquellos que infieren resultados a partir del conocimiento codificado por expertos humanos. En este caso, los sistemas no aprenden de los datos como en el aprendizaje automático, sino que razonan a partir de reglas, hechos y relaciones previamente definidas. Los sistemas expertos para diagnóstico médico y los motores de inferencia lógica, tanto deductiva como inductiva, son ejemplos de este enfoque. Estos sistemas también utilizan representaciones simbólicas del conocimiento, como ontologías, que permiten aplicar lógica formal para razonar sobre nuevas situaciones. Esta programación lógica e inductiva permite el uso de inferencias para resolver problemas complejos, como la búsqueda y optimización de soluciones. También se incluyen los motores de razonamiento simbólico que son capaces de procesar información a partir de un conjunto de reglas predefinidas.

Pasando a exclusiones, los considerandos de la AIA aclaran que la capacidad de inferencia de un sistema de IA trasciende así el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización[31]. En la práctica, esta capacidad de inferencia excluye

[31] Considerando 12 AIA.

los automatismos simples, las fórmulas, el software estático o la programación totalmente determinista (si *x*, entonces *y*)[32].

Esta capacidad de inferencia de los sistemas empleados para la personalización de las prácticas comerciales es utilizada por los sistemas de IA desarrollados por los principales proveedores de servicios de intermediación publicitaria (Alphabet, Meta y Amazon). Su actividad se basa en el empleo de complejos métodos de aprendizaje automático para gestionar múltiples funcionalidades, como las subastas de espacios publicitarios en tiempo real (*real time bidding*), los inventarios de anuncios, las mediciones de eficacia, la creación de anuncios mediante sistemas generativos o la elaboración y aplicación de perfiles publicitarios conforme a la información personal de sus usuarios[33].

El sistema de IA utilizado por estos proveedores no solo está presente en sus propios servicios, como las redes sociales, sino también en los servicios de terceros. De esta forma, cada uno de sus sistemas de IA publicitarios afecta al conjunto del mercado de intermediación publicitaria, controlado casi en su totalidad por los anteriores operadores[34]. Esta situación aumenta el impacto que puede derivar de posibles usos perniciosos de la capacidad de inferencia de los sistemas de IA, como ocurre con la explotación de adicciones y otras vulnerabilidades.

Esta capacidad de inferencia también posibilita la personalización y segmentación de prácticas comerciales en los asistentes virtuales y en los sistemas de IA conversacionales (como Alexa y ChatGPT). El sistema infiere, a partir de información sobre comportamientos previos del usuario, una gran cantidad de resultados de salida (como contenidos personalizados y recomendaciones) que, a su vez, retroalimentan la capacidad del sistema para deducir modelos o algoritmos que el sistema aplica tanto al usuario en cuestión como al resto de usuarios[35]. La capacidad de inferencia también se manifiesta en los sistemas de IA utilizados en los videojuegos *online* para personalizar el diseño del servicio, los anuncios mostrados, sus funcionalidades e, incluso, el desarrollo del juego conforme al perfil del usuario[36].

De forma general, cabe concluir que la mayoría de los sistemas utilizados con fines de personalización o segmentación de prácticas comerciales tienen cabida dentro de la definición de sistemas de IA de la AIA, puesto que presentan grandes capacidades de inferencia al basarse en complejas técnicas de aprendizaje.

---

[32] Maas, M. M., «Concepts in Advanced AI Governance: A Literature Review of Key Terms and Definitions», *Institute for Law & AI – AI Foundations Report 3,* octubre de 2023.

[33] Geradin, D. y Katsifis, D., «An EU competition law analysis…», *op. cit.*

[34] *Ibid.*

[35] Olmedo Peralta, E. «Entornos Informáticos…», *op. cit.,* pp.349-406.

[36] Boyan, B. «Modern Trends in Automatic Generation of Content for Video Games» *Serdica Journal of Computing*, 2019.

2.5. *La posible capacidad de influencia en entornos físicos o virtuales*

La última característica de los sistemas de IA, también de carácter optativo, es que los resultados de salida generados influyan en entornos físicos o virtuales. Conforme a las *Directrices sobre la definición de sistemas de IA*, ese elemento debe entenderse para enfatizar el hecho de que los sistemas de IA no son pasivos, sino que impactan activamente sobre los entornos en los que se despliegan. A nuestro entender, esta posibilidad de influencia justifica la aproximación por riesgo que caracteriza a la AIA. Como tendremos ocasión de exponer, aunque ciertas prácticas prohibidas no exigen la causación efectiva de un perjuicio considerable, sí que requieren, al menos, la probabilidad de provocación de un riesgo. Este riesgo —sostenemos— no debe ser meramente teórico, lo que pasa por exigir que el sistema pueda influir en entornos físicos o virtuales.

Las directrices aclaran que la referencia a entornos físicos o virtuales implica que la influencia de un sistema de IA puede proyectarse tanto sobre objetos físicos tangibles (por ejemplo, un brazo robot) como sobre entornos virtuales, incluidos los espacios digitales, los flujos de datos y los ecosistemas de software. Aunque las directrices no hagan referencia expresa a la influencia sobre personas, se entiende, bajo una interpretación contextual, que la capacidad de influencia también abarca este extremo, como bien se deriva de las prohibiciones sobre técnicas manipulativas, subliminales, explotadoras de vulnerabilidades o los preceptos referentes a los sistemas de IA de reconocimiento de emociones.

Aplicando esta característica a los sistemas de IA utilizados para personalizar prácticas comerciales, diversos estudios evidencian la capacidad de estos sistemas para influir en diversos entornos y decisiones individuales o grupales, como decisiones de compra[37]. Además, se ha puesto de manifiesto el diseño adictivo de ciertos servicios (como los videojuegos y las redes sociales)[38], configurando el fenómeno conocido como *dark patterns* o patrones oscuros basados en el círculo de la dopamina[39].

Recapitulando, esta influencia no es un requisito imprescindible para que el sistema en cuestión sea calificado como un sistema de IA a efectos del Reglamento. Ahora bien, bajo una aproximación por riesgo, los usos concretos de estos sistemas de IA y su capacidad para influir en ciertos entornos (particularmente de una forma dañina) sí que resultarán relevantes para calificar al mismo como un posible sistema prohibido a tenor de la AIA.

---

[37] Ienca, M. «On Artificial Intelligence and Manipulation», *Topoi* 42, 2023.
[38] Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair…», *op. cit.*
[39] *Ibid.*

II. PRÁCTICAS COMERCIALES PERSONALIZADAS MANIPULATIVAS O SUBLIMINALES DESARROLLADAS A PARTIR DE SISTEMAS DE IA. UN EXAMEN BAJO EL CATÁLOGO DE PROHIBICIONES DE LA AIA

El posible efecto restrictivo o condicionante sobre la autonomía de la voluntad de las personas ha constituido una de las principales preocupaciones a nivel ético y jurídico en diversos estudios sobre IA desarrollados en la última década[40]. Este riesgo, frecuentemente ejecutado mediante el uso de técnicas subliminales o manipulativas, lleva advirtiéndose como un problema que debía ser abordado por la política legislativa de la UE[41], lo que ha resultado en la inserción de prohibiciones absolutas sobre dichas prácticas de IA en el art. 5.1 AIA.

En respuesta a dichas preocupaciones, el art. 5.1.*a)* de la AIA incluye en el catálogo de prácticas prohibidas «la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que transciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas».

La prohibición se configura sobre seis elementos cumulativos, a saber: *a)* la actividad comprendida es la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA; *b)* la práctica debe valerse de técnicas subliminales que transciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas; *c)* el objetivo o el efecto debe ser alterar de manera sustancial el comportamiento de una persona o un colectivo de personas; y *d)* debe mermar de forma apreciable la capacidad de tomar una decisión informada; *e)* provocar la toma de una decisión que de otro modo

[40] Entre ellos, *vid.* European Commission, «Ethic Guidelines on Trusthworthy AI», 2019; Jobin, A., Ienca, M. y Vayena, E. «The global landscape of AI ethics guidelines», *Nature Machine Intelligence*, 2019, vol. 1, núm. 9, pp. 389-399; Prunkl, C. «Human autonomy in the age of artificial intelligence», *Nature Machine Intelligence*, 2022, vol. 4, núm. 2, pp. 99-101; Calvo, R.A. *et al.* «Supporting human autonomy in AI systems: A framework for ethical enquiry», in *Ethics of Digital Well-Being*, Springer, 2020, pp. 31-54;, Calvo, R.A. *et al.* «Autonomy in technology design», en *CHI'14 Extended Abstracts on Human Factors in Computing Systems*, 2014, pp. 37-40.

[41] European Commission, «AI Act Proposal explanatory memorandum», 2023, pp. 12-13.

no se hubiese tomado; y *f)* provocar o ser razonable que provoque perjuicios considerables a esa persona, a otra o a un colectivo de personas.

1. La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA. Sujetos obligados por las prohibiciones del art. 5 AIA

El primer requisito para que la práctica IA manipulativa o subliminal resulte prohibida es que se enmarque en una de las acciones relevantes comprendidas en el art. 5.1.a AIA, que son: la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA. Se cubren así tres acciones diferentes, cada una de ellas con una definición jurídica propia en el Reglamento.

A efectos de responsabilidad, conviene aclarar que, en vista de las acciones comprendidas, los sujetos obligados son los proveedores y responsables de despliegue, como bien aclaran las *Directrices sobre prácticas de IA prohibidas*[42]. En este sentido, el art. 3 de la AIA, en sus apartados 3 y 4 respectivamente, define al proveedor como «una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente», y al responsable de despliegue como «una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional». Esta última definición deja patente que la AIA pretende dejar fuera del ámbito de aplicación a los usos estrictamente personales de los sistemas de IA, lo que excluiría, así visto, a los consumidores y usuarios como sujetos obligados por las prohibiciones aquí analizadas.

Las prohibiciones analizadas en este apartado comparten la base común de las acciones relevantes consideradas. En este sentido, la primera acción introducida por la norma es la introducción en el mercado, definida como la primera comercialización en el mercado de la Unión de un sistema de IA o de un modelo de IA de uso general[43]. En nuestro ámbito sería la primera introducción de una IA destinada a la personalización de prácticas comerciales, desarrollando funciones como la elaboración de perfiles publicitarios (ya sean individuales o grupales), la asignación de una publicidad u otra conforme a tales perfiles,

---

[42] European Commission, *Communication to the Commission. Approval of the content of the draft…, op. cit.,* p. 10.

[43] Art. 3 (9) AIA.

la personalización de anuncios, o la personalización del diseño de un servicio digital. La práctica se valora con independencia de si el sistema de IA ha sido creado o no en la Unión, ya que lo relevante es que se comercialice por primera vez en el mercado de la UE[44].

La puesta en servicio es definida por su parte como el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista[45]. En este sentido, el responsable del despliegue es una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional[46]. Esto comprendería el suministro de sistemas de IA publicitarios a las empresas (responsables de despliegue) que en la actualidad presentan un mayor protagonismo en el mercado de la intermediación publicitaria: Meta, Alphabet y Amazon. La finalidad prevista comprende el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica[47].

La utilización de un sistema de IA no cuenta con una definición jurídica propia, si bien el principio de neutralidad tecnológica obliga a una interpretación abierta de este concepto, entendiendo que tiene cabida en el mismo cualquier uso de un sistema de IA, lo que comprendería la utilización de un sistema de IA para la promoción de productos y servicios en los mercados digitales y la personalización del diseño de los propios servicios. A título de ejemplo, cuando Meta pone su sistema publicitario a disposición de diversos anunciantes, estos últimos estarían utilizando el sistema de IA en el que se basa el servicio Meta Ads. Bajo una interpretación sistemática de la AIA, se entiende que esta solo se ocupa de establecer obligaciones relativas a la utilización profesional del sistema de IA, ya que la AIA excluye a los consumidores y usuarios del concepto de responsables de despliegue y, por ende, de las obligaciones aplicables a los mismos[48].

---

[44] La irrelevancia del lugar de fabricación o diseño del sistema de IA refleja el efecto extraterritorial que caracteriza a la AIA, dando lugar a una de las principales críticas dirigidas al Reglamento, sobre todo por parte de fabricantes chinos. *Vid.* Wang, Y. «Do not go gentle into that good night: The European Union's and China's different approaches to the extraterritorial application of artificial intelligence laws and regulations», *Computer Law & Security Review*, Volume 53, 2024.

[45] Art. 3 (11) AIA.

[46] Art. 3 (4) AIA.

[47] Art. 3 (12) AIA.

[48] Así se deriva del art 3 (4) AIA, que define al responsable de despliegue como «una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, *salvo cuando su uso se enmarque en una actividad personal de carácter no profesional*» (énfasis añadido).

2. La utilización de técnicas subliminales que transciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas

La AIA trata de minimizar los riesgos derivados del impacto que el uso de sistemas de IA puede producir sobre la autonomía de la voluntad de las personas afectadas por los servicios o productos que la utilizan. El caso analizado de Cambridge Analytica ya puso de manifiesto la relevancia de este problema. La posibilidad de afectar indebidamente la toma de decisiones de las personas a través de IA se extiende también a la personalización de las prácticas comerciales, cuya formulación se basa en la explotación de vastas cantidades de información sobre el comportamiento de los usuarios[49]. A nivel normativo, es necesario plantear si algunas de estas prácticas (comunes desde hace años en los mercados digitales) pueden resultar prohibidas al constituir riesgos calificados como inaceptables por la AIA.

La posibilidad de utilizar sistemas de IA que afecten de forma inaceptable a la capacidad de toma de decisiones de las personas ha dado lugar a la prohibición de dos acciones relevantes: *a)* la utilización de técnicas subliminales que transciendan la conciencia de una persona, y *b)* la utilización de técnicas deliberadamente manipuladoras o engañosas; siempre y cuando concurran los demás requisitos cumulativos exigidos en el art. 5 (1) *a)* AIA.

En la práctica, es posible que una misma técnica IA tenga cabida en ambos supuestos, al valerse de medios subliminales que sean al mismo tiempo deliberadamente manipuladores o engañosos[50]. Esta posible convergencia se aprecia también en los considerandos de la norma, que no llegan a aportar una diferenciación tajante de ambas acciones relevantes. El considerando 29 de la AIA se refiere así de forma conjunta a las técnicas posibilitadas por IA «para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socaven y perjudiquen su autonomía, su toma de decisiones y su capacidad de elegir libremente», sin llegar a diferenciar entre técnicas subliminales y técnicas manipulativas o engañosas.

Así las cosas, bajo una interpretación funcional, la cuestión esencial radica en si la práctica controvertida afecta de forma importante a la autonomía del destinatario de la publicidad para tomar una decisión, factor que encuentra ciertos denominadores comunes con la DPCD, si bien el supuesto de hecho del art. 5.1.*a)* de la AIA se extiende no solo

[49] Ienca, M. «On Artificial Intelligence…», *op. cit.*

[50] Boine, C., «The AI Manipulation Gap», *Emory International Law Review*, vol. 39, núm. 2 (2025).

a las prácticas comerciales hacia los consumidores, sino a cualquier práctica llevada a cabo mediante sistemas de IA que afecte a una persona o a un colectivo, con independencia de que sean o no consumidores. Aunque ambas acciones (técnicas subliminales y técnicas manipulativas) puedan resultar coincidentes y contengan la misma razón de ser, resulta conveniente analizar ambos conceptos por separado para determinar si la práctica es una práctica prohibida. Tampoco se debe perder de vista que no toda práctica subliminal tiene por qué ser manipulativa y que no toda práctica manipulativa se vale necesariamente de medios subliminales.

2.1. *La utilización de técnicas subliminales que transciendan la conciencia de una persona (física)*

La AIA no aporta una definición de técnicas subliminales, limitándose a ofrecer ejemplos de ciertos componentes subliminales utilizados por sistemas de IA, en concreto «estímulos de audio, imagen o vídeo que las personas no pueden percibir —ya que dichos estímulos trascienden la percepción humana»[51]. A todas luces, aunque el Reglamento extienda su protección a las personas físicas y jurídicas, el art. 5.1.*a)* AIA se acota exclusivamente a las personas físicas, puesto que son las únicas que presentan una conciencia que pueda ser afectada, a lo que se une la alusión a técnicas que transciendan la percepción humana, lo que excluiría, igualmente, el uso de técnicas subliminales que afecten a animales. Siguiendo las anteriores anotaciones, la conceptualización más cercana aportada por la AIA exigiría determinar si la técnica transciende la conciencia de una persona a través de señales o estímulos que sean imperceptibles por el ser humano, examen que debe realizarse casuísticamente[52].

Conforme a las *Directrices sobre prácticas de IA prohibidas*, existen varias técnicas subliminales que pueden ser utilizadas por los sistemas de IA, que no están necesariamente prohibidas, salvo que se

---

[51] Considerando (29) AIA. La preocupación del legislador comunitario sobre el uso de técnicas subliminales encuentra ciertos precedentes en la Directiva (UE) 2018/1808 por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (en adelante, DSCA). En su art. 9.1.*b)* prohíbe las comunicaciones comerciales basadas en técnicas subliminales, si bien no llega tampoco a describir qué debemos entender por técnicas subliminales. A nivel internacional, esta preocupación por el uso de medios subliminales viene de largo. A título de ejemplo, la publicidad subliminal fue prohibida en el art. 13(2) Convenio europeo sobre la televisión transfronteriza, Serie de Tratados Europeos – núm. 132 (5 de mayo de 1989) y art. 10(3) Comunidades Económicas Europeas, Directiva 89/552/CEE del Consejo (Directiva «Televisión sin fronteras»), *DO* L 298/23-30 (17 de octubre de 1989).

[52] Cohen, T. «Regulating Manipulative Artificial Intelligence», *SCRIPTed – A Journal of Law, Technology & Society*, vol. 20, núm. 1, febrero 2023.

cumplan todas las condiciones previstas en el art. 5.1.*a)* de la AIA. Entre estos ejemplos se incluyen los mensajes subliminales visuales, en los que el sistema presenta imágenes o texto que parpadean brevemente durante la reproducción de un video, siendo visibles solo a nivel técnico, pero demasiado rápidos para ser registrados conscientemente. De manera similar, las directrices también mencionan que los mensajes subliminales auditivos implican sonidos o mensajes verbales emitidos a volúmenes bajos o enmascarados, que afectan al oyente sin que sea consciente de ellos.

Las directrices también advierten que existen estímulos táctiles subliminales que inducen sensaciones físicas sutiles, capaces de influir en el comportamiento o estado emocional sin que la persona sea consciente de su percepción. Advierten, igualmente, sobre señales subvisuales y subauditivas que se presentan de manera completamente indetectable para los sentidos humanos, como imágenes que parpadean demasiado rápido o sonidos a volúmenes inaudibles. Otra técnica mencionada es el uso de imágenes incrustadas, donde un sistema puede esconder imágenes dentro de otros contenidos visuales que no se perciben conscientemente, pero que aún pueden influir en el comportamiento. También se cita la distracción *(misdirection)*, mediante la cual se enfoca la atención en ciertos estímulos para evitar que se perciban otros, aprovechando sesgos cognitivos y vulnerabilidades de atención. Por último, las directrices se refieren a la manipulación temporal, afirmando que altera la percepción del tiempo en las interacciones del usuario, generando efectos como impaciencia y dependencia.

La doctrina, por su parte, también se ha pronunciado sobre el impacto subliminal de determinadas técnicas de IA. HACKER aporta como ejemplo las señales subconscientes insertadas en vídeos por una IA que incitan a comportamientos violentos[53]. GRADY cita una multiplicidad de casos prácticos, como son: un robot humanoide que utiliza el lenguaje corporal para transmitir amabilidad; un complemento del navegador que emplea determinadas ondas luminosas para seguir y mejorar la atención del usuario; un tratamiento de spa que utiliza aromas generados por inteligencia artificial para calmar a los clientes; un reloj inteligente que motiva a los usuarios a hacer ejercicio durante más tiempo mediante imágenes inspiradoras; un wearable diseñado para hacer dieta que emplea vibraciones imperceptibles para reducir la sensación de hambre; o un auricular de meditación que estabiliza sutilmente la sensación de movimiento del usuario[54].

Si bien —como evidencian los anteriores ejemplos de la Comisión y de la doctrina— no toda técnica subliminal presenta necesariamente

---

[53] Hacker, P. «Manipulation by algorithms…», *op. cit.*

[54] Grady, P. «EU's AI Act Resurrects Subliminal Messaging Panic», *Center for Data Innovation*, 21 de octubre de 2022.

connotaciones o repercusiones negativas, ciertos usos concretos pueden derivar en efectos perjudiciales para las personas físicas en diversos ámbitos (como sus decisiones electorales, su estado de salud o su comportamiento económico).

Ya empiezan a advertirse algunos usos negativos en el ámbito publicitario. A título de ejemplo, hay estudios que sugieren que el uso comercial de la incubación de sueños o *dream incubation* (es decir, la presentación de estímulos antes o durante el sueño para afectar a su contenido) se está probando en numerosos estudios de marketing para encontrar formas de alterar e impulsar el comportamiento de compra[55]. De esta forma, la presentación de anuncios personalizados en plataformas como YouTube justo antes de que el usuario se vaya a dormir podría tener un efecto subliminal en su comportamiento económico.

Siguiendo con el marco de las prácticas comerciales personalizadas, algunas técnicas subliminales empleadas por IA también podrían tener un papel importante en el diseño adictivo de ciertos servicios digitales (*hiper-engaging dark patterns*). Estas técnicas presentan un especial protagonismo en los videojuegos en línea, caracterizados por explotar el círculo de la dopamina en cada usuario[56] y por emplear otras técnicas que transcienden las capacidades cognitivas del usuario, como el uso de luces, colores y sonidos imperceptibles al oído durante el juego[57]. El legislador parece poner un foco especial de atención en estos servicios, en vista de que el considerando 29 de la AIA hace referencia expresa al uso de técnicas de realidad virtual —mayormente utilizadas en videojuegos, pero cuyo uso se está extrapolando a otros entornos como las redes sociales—, advirtiendo que las mismas «permiten un mayor grado de control acerca de qué estímulos se presentan a las personas, en la medida en que pueden alterar sustancialmente su comportamiento de un modo que suponga un perjuicio considerable».

La necesidad de abordar técnicas que afecten de forma encubierta al comportamiento de los usuarios también se ha manifestado en el *Fitness Check 2024*. El informe señala diversas técnicas utilizadas en plataformas digitales que pueden fomentar comportamientos adictivos, afectando tanto a la interacción del usuario como a su bienestar. Una de estas técnicas es la reproducción automática, mediante la cual se reproduce contenido de forma secuencial y continua sin necesidad de que el usuario intervenga, eliminando así la toma autónoma de de-

---

[55] Horowitz, A.H.; Stickgold, R. y Zadra, A. «Inside your dreamscape», *Aeon*, 19 noviembre 2021.

[56] Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair…», *op. cit.,* pp.1000-1016.

[57] Albarrak, L., Metatla, O. y Roudaut, A. «Exploring the influence of subliminal stimulus type and peripheral angle on the priming effect» *International Journal of Human – Computer Studies* 151, 2021, pp. 1-17.

cisiones y, potencialmente, fomentando la adicción al servicio. De manera similar se refiere al *pull-to-refresh*, que permite a los usuarios recargar la interfaz deslizando hacia abajo para obtener nuevos contenidos. Este mecanismo, al ofrecer una recompensa variable, explota las mismas vulnerabilidades psicológicas que impulsan las adicciones al juego, creando un ciclo de expectativas y gratificación impredecible. Asimismo, el desplazamiento infinito permite la aparición automática y continua de nuevos contenidos a medida que el usuario navega por la página. Esta técnica también está vinculada a la recompensa variable, ya que genera la ilusión de que siempre habrá contenido interesante disponible, aunque no se pueda predecir la calidad del siguiente elemento mostrado.

Otro conjunto de técnicas descritas en el *Fitness Check 2024* incluye la inversión social, la cual se manifiesta en métricas como el número de reacciones, seguidores y visitas. Estas métricas pueden inducir a los usuarios a invertir tiempo, dinero y otros recursos en la plataforma, fomentando la idea de que deben continuar interactuando con el servicio para no perder sus avances. Las redes sociales, al estructurar estas recompensas de forma que incentiven el uso constante de la plataforma, logran mantener al usuario conectado. Además, las compras dentro de aplicaciones o juegos, que incluyen monedas virtuales, potenciadores y contenido exclusivo, suelen requerir pequeñas cantidades de dinero real para acceder a elementos del juego. El diseño de estas compras, con su ritmo rápido, repetibilidad y elementos aleatorios, como las «cajas de botín», ha sido comparado con el de las llamadas máquinas tragaperras, lo que ha suscitado preocupaciones sobre su impacto psicológico.

Otra de las técnicas identificadas por el informe es la gamificación. Esta práctica implica la incorporación de elementos de juegos en entornos no lúdicos, como en aplicaciones de entrenamiento o juegos para móviles. Su funcionamiento se basa en la recompensa a los usuarios por sus logros, incentivando su comportamiento y fomentando la interacción continua con la plataforma. La Comisión Europea ha manifestado su preocupación por los riesgos derivados de la gamificación, especialmente a raíz de la investigación abierta a la plataforma Temu por posible infracción de la DSA[58]. La investigación pone de relieve los riesgos asociados con el diseño adictivo de ciertos servicios, incluidos los programas de recompensas similares a los de los juegos, que pueden tener consecuencias negativas para el bienestar físico y mental de los usuarios.

[58] Comisión Europea, «La Comisión incoa un procedimiento formal contra Temu en virtud de la Ley de Servicios Digitales», comunicado de prensa, 31 octubre de 2024.

El nexo entre estos mecanismos potenciadores de adicciones ejecutados a través de sistemas de IA y la merma de la autonomía del usuario para la toma de ciertas decisiones (como las decisiones de compra en el servicio o el número de horas dedicadas al mismo) resulta evidente. También lo es su auge actual. Los sondeos realizados por la Comisión Europea revelan que en los últimos 5 años el uso de técnicas subliminales basadas en IA con propósitos comerciales ha aumentado en un 67,7 por ciento. El uso exponencialmente mayor de estas prácticas justifica su tratamiento en la AIA[59].

Ahora bien, bajo la literalidad de la norma puede ponerse en entredicho si las técnicas anteriormente expuestas pueden ser consideradas «subliminales», en el sentido de la AIA o, dicho de otra forma, si tales técnicas IA son realmente imperceptibles por sus destinatarios. A título de ejemplo, el desplazamiento infinito de Instagram es un estímulo cognitivamente perceptible por sus usuarios, siendo lógico asumir que los usuarios son mínimamente conscientes de que la lista de vídeos o contenidos sugeridos es inacabable, si bien es cierto que la explotación de adicciones a través de estos estímulos reduce (pero no elimina absolutamente) su percepción con respecto al servicio o sus funcionalidades[60].

En consecuencia, muchas de estas técnicas podrían no ser consideradas subliminales en el sentido de la AIA, ya que no rebasan o transcienden puramente la conciencia de sus destinatarios (al resultar perceptibles por los mismos). Esta aproximación ha dado lugar a críticas sobre la caracterización del término *subliminal* en el nuevo Reglamento, indicando que hubiese sido más deseable entender estas técnicas de una forma más flexible[61]. Ahora bien, desde un punto de vista funcional, esta falta de flexibilidad puede salvarse hasta cierto punto si aplicamos un examen de dos pasos sobre el art. 5.1.*a)* AIA.

El primer paso consistiría en determinar si el sistema de IA hace uso de técnicas claramente subliminales, en el sentido de que las mismas sean imperceptibles para los humanos. Un ejemplo sería el uso de luces, sonidos y otros estímulos que el usuario no sea capaz de percibir debido a limitaciones cognitivas. Estos estímulos podrían tener un especial protagonismo en el diseño adictivo de ciertos servicios digitales. Si bien ciertas técnicas subliminales insertas en las plataformas en línea pueden quedar cubiertas por la prohibición de *dark patterns*

---

[59] Whittle, M. *et al., Study to support the Fitness Check of EU…, op. cit.,* p. 39.

[60] Krook, J. «Manipulation and the AI Act: Large Language Model Chatbots and the Danger of Mirrors», *SSRN Electronic Journal*, 2024.

[61] Bermúdez, J. P. *et al.*, «What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence», *2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, 2023, pp. 1-10.

del art. 25.1 de la DSA[62], la prohibición de técnicas IA subliminales de la AIA podría ser especialmente relevante para abordar prácticas desarrolladas en servicios no cubiertos por la DSA (como los videojuegos en línea).

El segundo paso se aplicaría en caso de que quede en duda el carácter subliminal de la práctica IA, al emplear estímulos o técnicas que no sean estrictamente imperceptibles cognitivamente, pero que afecten a la capacidad de decidir de los destinatarios de una forma reprochable bajo la aproximación por riesgo de la AIA. Este segundo paso consistiría en examinar si concurre la segunda acción relevante contemplada por el art. 5.1.*a)* AIA, es decir, el uso de técnicas deliberadamente manipuladoras o engañosas[63].

2.2. *La utilización de técnicas deliberadamente manipulativas o engañosas*

La segunda acción relevante contemplada por el art. 5.1.*a)* de la AIA es la utilización de técnicas deliberadamente manipulativas o engañosas a través de sistemas de IA. Como adelantábamos, esta prohibición puede ser particularmente relevante cuando se utilicen sistemas de IA que afecten sustancialmente a la autonomía de las personas, pero no se sirvan claramente de técnicas subliminales. En lo que aquí nos atañe, las técnicas IA que pueden guardar más relevancia serán las «deliberadamente manipulativas», en vista de que las prácticas comerciales aquí analizadas se presentan como especialmente problemáticas no por su falta de transparencia o información (configurando su posible carácter engañoso), sino por la creación o explotación inaceptable de vulnerabilidades para afectar a la toma de decisiones comerciales[64].

Las técnicas deliberadamente manipulativas no están definidas en la AIA, si bien las *Directrices sobre prácticas de IA prohibidas* señalan que deben entenderse como técnicas diseñadas o que tienen como objetivo influir, alterar o controlar el comportamiento de un individuo de una manera que socave su autonomía individual y sus decisiones libres. Las directrices señalan que las técnicas manipulativas suelen estar diseñadas para explotar sesgos cognitivos[65], vulnerabilidades

---

[62] Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair…», *op. cit.*

[63] Bongard-Blanchy, K. *et al.*, «"I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" – Dark Patterns from the End-User Perspective» in *Proceedings Of The 2021 Acm Designing Interactive Systems Conference 763*, 2021.

[64] Dicho de otra forma, la reprochabilidad de estas prácticas comerciales no se sitúa en la falta de transparencia o de información, sino en el uso de información reveladora de vulnerabilidades para ejercer una influencia comercial que pueda ser ilícita bajo la normativa actual.

[65] Véase aquí, de nuevo, el creciente protagonismo de los sesgos cognitivos en el marco de la UE, manifestado en la ya analizada Sentencia del Tribunal de Justicia de 14 de noviembre

psicológicas o factores situacionales que hacen que los individuos sean más susceptibles a la influencia. Debido a su adaptabilidad, los sistemas de IA también son capaces de responder bien a las circunstancias o vulnerabilidades individuales de una persona, aumentando la efectividad e impacto de la manipulación a gran escala.

Para deslindar con precisión el ámbito objetivo de esta prohibición (el uso de técnicas IA deliberadamente manipulativas) debemos dar respuesta a dos cuestiones previas: *a)* la distinción entre técnicas IA que sean manipuladoras y otras que sean meramente persuasivas, y *b)* cuándo las mismas se llevan a cabo deliberadamente.

Comenzando por la primera incógnita, el concepto *manipulación* y sus intentos de caracterización cuentan con una larga presencia en la doctrina jurídica y económica. Ya en 1999, HANSON y KYSAR acuñaron la noción de «manipulación del mercado» para describir cómo las empresas explotan las limitaciones cognitivas de los consumidores[66]. El movimiento de manipulación del mercado (defendido por un gran número de autores) complementa y desafía al derecho y a la economía evidenciando que las personas no siempre se comportan en su mejor interés, como suponen los modelos económicos tradicionales[67]. Suponen, en consecuencia, otorgar un mayor protagonismo a los factores psicológicos en la definición de los comportamientos en el mercado. Por ello, las ideas de este movimiento justifican que el ser humano se comporta de una forma *predeciblemente irracional*[68].

Siguiendo este argumento, cualquier política legislativa que se diseñe asumiendo el comportamiento completamente racional de los individuos en los mercados digitales estaría abocada a fracasar, mientras que aquellas normas que tengan en cuenta las limitaciones cognitivas y los prejuicios humanos tendrán una mayor capacidad para predecir sus resultados y mejorar la elaboración de políticas en general[69]. Un ejemplo práctico de esta doctrina serían las limitaciones del actual concepto de consumidor medio. Si asumimos que el consumidor medio es siempre razonablemente informado, atento y perspicaz, caeremos en el riesgo de ignorar que a menudo carece de estos caracteres, actuando de una manera irracional que puede ser predecible y explotable por el algoritmo publicitario con fines contrarios a su mejor interés.

---

de 2024, asunto C-646/22, *Compass Banca SpA,* ECLI:EU:C:2024:957 (conclusión tercera).

[66] Hanson, J. D. y Kysar, D. «Taking Behavioralism Seriously: Some Evidence of Market Manipulation», *112 Harv. L. Rev. 1420,* 1999, pp.1564-65.

[67] Jolls, C. *et al.* «A Behavioral Approach to Law and Economics*», 50 Stan. L.rev.* 1471, 1998.

[68] Ariely, D. *Predictably irrational: the hidden forces that shape our decisions,* HarperCollins, 2010.

[69] Calo, R. «Digital market manipulation», *82 George Washington Law Review 995*, 2014, versión *online*.

Aunque advertíamos en otro lugar que esta reformulación del consumidor medio como consumidor irracional presenta el riesgo de ser excesivamente paternalista e incierta si no se modula con cautela, puede resultar positivo que la AIA considere la manipulación como una de sus prácticas prohibidas, al componer una alternativa que permita abordar la explotación por sistemas de IA de irracionalidades predecibles. En este punto, la ausencia de una definición jurídica de las técnicas IA manipulativas puede ser tanto una virtud (al ser un término tecnológicamente neutro y flexible) como un vicio (al presentar graves riesgos de inseguridad jurídica).

Si bien el tenor de la AIA no aporta una definición concreta de las técnicas manipulativas, el considerando 29 indica que éstas «pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente»[70]. En otras palabras, el núcleo de las técnicas manipulativas se sitúa en la merma de la capacidad para tomar decisiones libremente, núcleo que encuentra evidentes denominadores comunes con la DPCD y la LCD, si bien estas últimas se ocupan de la toma de decisiones con respecto a un producto o servicio, ocupándose exclusivamente de la afección del comportamiento económico del consumidor.

La manipulación como merma de la autonomía encuentra claros precedentes en la doctrina económica y jurídica, que caracteriza la manipulación sobre dos factores principales: *a)* el intento de subvertir la toma de decisiones consciente mediante una influencia oculta y *b)* la explotación de vulnerabilidades cognitivas, emocionales o de otro tipo en la toma de decisiones[71]. Ambos factores encuentran sus equivalentes en la AIA en: *a)* la intencionalidad manipulativa y *b)* la afección de la autonomía de las personas[72].

Bajo una interpretación funcional, la explotación de vulnerabilidades podría servir para diferenciar aquellas prácticas IA que afecten a la autonomía de una forma lícita —lo que tradicionalmente se viene conociendo como *persuasión*— de aquellas que sean ilícitas por suponer un riesgo inaceptable —al servirse de técnicas IA de *manipulación*—[73].

---

[70] Considerando 29.

[71] Susser, D. *et al.* «Online Manipulation: Hidden Influences in a Digital World», *Georgetown Law Technology Review,* 2019.

[72] Art. 5.1 y considerando 29 AIA.

[73] Si bien las distinciones filosóficas entre la persuasión y la manipulación exceden del presente trabajo (ocupado exclusivamente de la manipulación en las prácticas comerciales personalizadas), conviene subrayar que el debate sobre la línea que separa ambos conceptos precede de largo al movimiento de la manipulación de los mercados digitales. A título de ejemplo, Aristóteles ya diferenciaba en su *Retórica* a la persuasión como una forma ética de influencia (a diferencia de la manipulación), señalando que la persuasión se basaba en tres modos de prueba: el

Si asociamos los componentes aportados por la AIA y por la doctrina, podríamos establecer cuatro indicios para calificar a una práctica desarrollada por medio de IA como manipulativa:

1. *La asimetría de resultados*. La manipulación implica comportamientos que producen resultados positivos para el manipulador (como el beneficio personal o el económico) y resultados negativos para el manipulado (como el perjuicio físico, psicológico, financiero o la realización de acciones que no redundan en beneficio de la víctima)[74]. Esta asimetría también es exigida por el art. 5.1.*a)* de la AIA que, como veremos más adelante, exige la provocación de perjuicios considerables a esa persona, a otra o a un colectivo de personas.

2. *La falta de transparencia*. Las distintas teorías de manipulación coinciden en que esta se configura como una forma de influencia generalmente encubierta y difícil de detectar[75]. El considerando 29 de la AIA adopta una aproximación similar al señalar que las personas no son realmente conscientes de dichas técnicas o, cuando lo son, pueden seguir siendo engañadas o no pueden controlarlas u oponerles resistencia. En otras palabras, la norma no exige una imposibilidad absoluta de percibir dicha manipulación, lo que permitiría acoger prácticas comerciales que resultan problemáticas no por falta de información o transparencia, sino por el uso indebido de una influencia derivada del análisis de datos y vulnerabilidades del destinatario (por ejemplo, los patrones adictivos o la personalización de precios).

3. *La violación de la autonomía*. La doctrina considera que el carácter no transparente de la práctica resulta en una violación de la autonomía personal del individuo o del grupo manipulado, mermando, o incluso anulando, la capacidad del sujeto afectado para tomar decisiones libres[76]. La AIA se sitúa en la misma línea, al señalar que las prácticas manipulativas llevan a las personas a que adopten comportamientos no deseados o a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente[77].

4. *La intencionalidad*. La última característica señalada por el común de las teorías sobre la manipulación del mercado implica la intención manipulativa, entendida esta como la intención de ejercer una in-

---

logos (el uso de argumentos lógicos), el *ethos* (la credibilidad y autoridad del orador) y el *pathos* (el atractivo emocional del argumento). Sobre distinciones filosóficas entre manipulación y persuasión, *vid.* Dileo, D. «Aristotle's manipulative maxim». *Rev Pol 82*(3), 2020, pp. 371-392.

[74] Ienca, M. «On Artificial Intelligence…», *op. cit.*

[75] *Ibid.*

[76] Saas, R. «Manipulation, Algorithm Design, and the Multiple Dimensions of Autonomy. *Philos. Technol,* 2024.

[77] Considerando (29) AIA.

fluencia indebida sobre el comportamiento o el sistema de creencias de otra persona[78].

Como advertíamos, la intencionalidad constituye la segunda incógnita interpretativa para determinar la concurrencia de la acción prohibida por el art. 5.1.*a)* AIA. Aunque se constate que la técnica IA presenta los caracteres para ser considerada manipulativa, la norma va un paso más allá, al exigir que dicha manipulación sea intencionada. Así se desprende de forma expresa del literal de la prohibición, al referirse a la utilización de técnicas *deliberadamente* manipuladoras[79]. La prueba de esta intencionalidad, por otro lado, exigiría el uso de sistemas de IA explicables (en adelante, por sus siglas en inglés, *XAI)*[80], cuyo análisis excede del presente trabajo.

Para determinar si concurre una manipulación intencionada, es necesario apuntar que la intencionalidad mantiene acentuadas conexiones con la previsibilidad, como bien se concluye del considerando 29 de la AIA, al señalar que «no puede presuponerse la intención de alterar el comportamiento si la alteración es el resultado de factores externos al sistema de IA que escapan al control del proveedor o del responsable del despliegue, a saber, factores que no es lógico prever y que, por tanto, el proveedor o el responsable del despliegue del sistema de IA no pueden mitigar».

En consecuencia, la alteración del comportamiento debe ser previsible por el proveedor o el responsable del despliegue, identificado como el sujeto activo de la técnica manipulativa. Bajo un encuadre sistemático, es razonable afirmar que dicha previsibilidad mantiene fuertes conexiones con dos conceptos: *a)* la finalidad prevista del sistema de IA y *b)* su uso indebido razonablemente previsible.

La finalidad prevista es definida por el art. 3.12 AIA como «el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica». En lo que aquí nos ocupa, la intención de alterar el comportamiento del destinatario de la práctica comercial personalizada a través de IA no se presume, si bien dicha intencionalidad podría justificarse a raíz de la información facilitada para describir la finalidad prevista.

Dado que sería cuanto menos esperpéntico encontrarnos ante un escenario en el que la documentación técnica aportada por el proveedor

---

[78] Ienca, M. «On Artificial Intelligence…», *op. cit.*

[79] Art. 5 (1) *a)* AIA (énfasis añadido).

[80] Malgieri, G. y Pasquale, F.A., «From Transparency to Justification: Toward Ex Ante Accountability for AI», *Brooklyn Law School, Legal Studies Paper No. 712, Brussels Privacy Hub Working Paper*, núm. 33, 2022.

admita expresamente la intención manipuladora entre sus finalidades previstas, dicha intencionalidad suele poder colegirse indirectamente a partir de factores como las instrucciones de uso, los datos de entrada utilizados, las declaraciones de promoción de venta y demás documentación técnica. En otras palabras, la alteración del comportamiento puede ser una finalidad explícita o implícita en el sistema de IA, ya que la aplicabilidad de las prohibiciones de la AIA no puede hacerse depender exclusivamente de la información aportada por el proveedor o responsable de despliegue.

Google Analytics podría ser un buen ejemplo de personalización de las prácticas comerciales. El sistema de IA en el que se basa permite a los medios publicitarios rastrear y conseguir información sobre quiénes visitan sus sitios web (como los datos de localización, la página web de procedencia, las páginas visitadas previamente, el tiempo de permanencia en el sitio web y las acciones o interacciones realizadas en la misma)[81][82]. Si bien es lógico que entre las finalidades previstas —o, al menos, declaradas— de su sistema no conste específicamente la utilización de técnicas manipulativas, es razonable que dichas funcionalidades revelen el potencial de influir en la capacidad de decisiones de los usuarios afectados de una forma en la que se socave su autonomía. Así las cosas, el proveedor o responsable de despliegue (Alphabet) no podría ampararse en la imprevisibilidad de su uso manipulativo o en factores completamente externos que escapan a su control para evitar que la práctica IA se califique como prohibida.

En vista de que la mayoría de los sistemas de IA utilizados con fines de personalización de prácticas comerciales presentan el ánimo directo de influir en la toma de decisiones comerciales, es poco probable que sus respectivos proveedores o responsables de despliegue puedan alegar con fundamento que el uso manipulativo era imprevisible. Aun en el caso de que se pruebe que la finalidad prevista no era la manipulación, el proveedor o responsable de despliegue quedaría asimismo sujeto a las exigencias previstas por la AIA con respecto a los usos indebidos razonablemente previsibles, lo que nos lleva al segundo concepto en el que se conectan la intencionalidad y la previsibilidad.

El art. 3.13 de la AIA define el uso indebido razonablemente previsible como «la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un

---

[81] Google, «How Google Analytics works», *https://support.google.com/analytics/answer/12159447*.

[82] Algunos estudios evidencian que Google Analytics está presente en el 62 por ciento de las 100 000 páginas web más populares a nivel mundial, impacto que merece estudiar detenidamente el posible carácter manipulativo de las prácticas llevadas a cabo mediante este sistema. *Vid.* Builtwith Pty Ltd., «Google Analytics Usage Statistics», disponible en *https://trends.builtwith.com/analytics/Google-Analytics*.

comportamiento humano o una interacción con otros sistemas, incluidos otros sistemas de IA, razonablemente previsible». Retomando ejemplos anteriores, aunque Alphabet alegue que el sistema de IA de *Google Analytics* no tiene como finalidad manipular la toma de decisiones económicas de los usuarios, es razonablemente previsible que los operadores involucrados en la cadena de intermediación publicitaria puedan utilizar este sistema con fines manipulativos, teniendo en cuenta las finalidades previstas y declaradas por la propia Alphabet con respecto al servicio.

Concluyendo, es probable que un sistema de IA que explote datos personales para personalizar prácticas comerciales guarde las notas necesarias para ser utilizado de una forma deliberadamente manipulativa, bien porque *a)* su finalidad prevista ampara (implícita o explícitamente) un uso manipulativo, y/o *b)* su utilización de forma manipulativa era razonablemente previsible por parte del proveedor o del responsable del despliegue; si bien es cierto que la formulación de guías técnicas y jurídicas por parte de instituciones y grupos de expertos contribuiría a definir con mayor seguridad el concepto de técnicas manipulativas en el marco de la AIA.

Ahora bien, la utilización deliberadamente manipulativa de un sistema de IA no implica, por sí misma, que la práctica quede prohibida bajo la AIA[83]. Como advertíamos, se exige la concurrencia de otra serie de criterios cumulativos que se analizan seguidamente.

3. Su objetivo o efecto: la alteración sustancial del comportamiento de una persona o un colectivo de personas

El art. 5.1.*a)* de la AIA exige que la técnica subliminal, manipuladora o engañosa tenga como objeto o efecto alterar de manera sustancial el comportamiento de una persona o un colectivo de personas. En lo que aquí nos atañe, este requisito se caracteriza por dos factores, *a)* la alternatividad entre el objetivo y el efecto, *b)* la exigencia de una alteración *sustancial* del comportamiento de una persona o un colectivo de personas.

3.1. *La alternatividad entre «objetivo» o «efecto», en la alteración comportamental*

La alternatividad entre los términos «objetivo» o «efecto» revela que no es necesario que el sistema de IA quede diseñado de forma que su finalidad sea una alteración comportamental, sino que bas-

[83] Barrio Andrés, M. *Objeto, ámbito de aplicación…, op. cit.,* pp. 30-40.

ta con que este efecto se produzca en la práctica, como confirman las *Directrices sobre prácticas de IA prohibidas*. Dicha alternatividad resulta coherente con argumentos que exponíamos previamente, por los cuales la intencionalidad manipulativa se identifica más con una previsibilidad razonable de la alteración del comportamiento, que con una intencionalidad manipulativa *stricto sensu*, en vista de los altos requisitos probatorios que la misma conllevaría. Esta interpretación conciliadora sería la más garante de los derechos y libertades de las personas físicas, ya que ampararía inicialmente sistemas de IA en los que:

1) La técnica es deliberadamente manipulativa y tiene el objetivo de alterar sustancialmente el comportamiento de una persona o de un colectivo. En este supuesto podrían encuadrarse determinados *dark patterns* que explotan vulnerabilidades a través de IA con el objetivo de crear o fomentar la adicción del usuario al servicio digital. En consecuencia, este precepto sería particularmente útil para abordar *dark patterns* manipulativos que no queden amparados por la DSA por no introducirse en plataformas en línea (como es el caso de los videojuegos *online*).

2) La técnica no es deliberadamente manipulativa o esta intencionalidad no resulta clara a nivel probatorio, pero su uso manipulativo era razonablemente previsible por el proveedor o el responsable del despliegue, y el efecto real producido por dicha técnica es la alteración sustancial del comportamiento de una persona o un colectivo. Este supuesto serviría como cláusula de cierre para abarcar ciertos supuestos no amparados claramente por el caso anterior. En otras palabras, aunque el proveedor o responsable de despliegue alegue que el diseño de un servicio a través de IA no tiene una intención manipulativa, dicha argumentación sería irrelevante si la alteración del comportamiento era previsible y el efecto en la práctica es dicha alteración del comportamiento.

En el caso de las técnicas subliminales, la interpretación de este requisito daría cobertura a los siguientes escenarios:

1) El sistema de IA se vale de sistemas subliminales con el objetivo de alterar sustancialmente el comportamiento de una persona o de un grupo de personas. Por ejemplo, Facebook Australia se jactó de su capacidad para inferir los estados emocionales de sus usuarios jóvenes —como el estrés, la ansiedad y el nerviosismo—, con el objeto de dirigirse a ellos a través de estímulos inconscientes en momentos de inseguridad, como cuando están interesados en hacer ejercicio y perder peso[84]. Este caso, que fue muy criticado, podría afrontarse en la actualidad desde la prohibición de técnicas subliminales del art. 5.1.*a)* AIA.

[84] Davidson, D., «Facebook Exploits “Insecure” to Sell Ads», *The Australian*, 2017

Lo mismo sucedería con el uso de sistemas de IA que presenten anuncios personalizados justo antes de dormir para afectar el contenido de los sueños (incubación de sueños), influyendo de manera imperceptible en las decisiones de compra[85].

2) El sistema de IA se vale de sistemas subliminales, produciendo como efecto la alteración sustancial del comportamiento de una persona o de un grupo de personas. Esta segunda previsión actuaría como punto de anclaje para aquellos casos en los que el objetivo no sea claramente la alteración del comportamiento, pero en los que se produce dicho efecto.

En el contexto de las prácticas comerciales personalizadas que emplean técnicas IA manipulativas o subliminales, sería controvertido sostener que prácticas como las anteriormente mencionadas no tienen como objetivo deliberado la alteración del comportamiento o, al menos, que esta alteración no fuese razonablemente previsible. No obstante, la inclusión de una segunda opción (el *efecto* de alterar el comportamiento) puede resultar eficaz para abordar aquellos supuestos en los que la intencionalidad sea difícil de acreditar, siempre que se constate la existencia de una alteración comportamental que presente suficiente entidad.

3.2. *La alteración sustancial del comportamiento*

Para que la práctica tenga la consideración de prohibida, el art. 5.1.*a)* AIA exige que la técnica en cuestión tenga como objetivo o efecto alterar *de manera sustancial* el comportamiento de una persona o un colectivo de personas. Así las cosas, la norma parece excluir aquellas técnicas que tengan como objeto o efecto unas alteraciones comportamentales mínimas o irrelevantes. En lo que aquí nos atañe, este requerimiento nos lleva a cuestionar cuándo una práctica comercial basada en IA tiene como objetivo o efecto una alteración sustancial del comportamiento.

En cuanto al requisito de que dicha alteración sea sustancial, las *Directrices sobre prácticas de IA prohibidas* sostienen que debe entenderse como la reducción significativa de la capacidad de una persona para adoptar decisiones informadas y autónomas, lo que da lugar a que dicha persona adopte comportamientos o tome decisiones que, en condiciones normales, no habría adoptado[86]. Las Directrices aclaran que este menoscabo debe exceder los efectos meramente marginales o insignificantes, dando lugar a una distorsión sustantiva o un obstáculo relevante en el proceso de toma de decisiones y en el ejercicio de la

[85] Horowitz, A. H., Stickgold, R., Zadra, A. «Inside your dreamscape…», *op. cit.*
[86] Whittle, M. *et al., Study to support the Fitness Check of EU…, op. cit.,* pp. 18-28.

libre determinación, incluidos los procesos de formación de opiniones y creencias. En este sentido, sostienen que la noción de *alteración sustancial* implica un grado de coacción, manipulación o engaño que supera los límites de la persuasión legítima (anteriormente analizada) y que no se comprende en el ámbito de aplicación de la prohibición.

Esta alteración sustancial se formula parcialmente como un requisito de peligro o de riesgo. Dado que la prohibición prevé que la alteración sustancial sea alternativamente un efecto o un objetivo de la técnica IA en cuestión, entrarán dentro de su ámbito de aplicación aquellas técnicas IA que presenten la mera aptitud para distorsionar significativamente dicho comportamiento, sin que resulte necesaria su distorsión efectiva.

Esta configuración como ilícito de riesgo recuerda claramente a la cláusula general de deslealtad prevista en la DPCD y en la LCD. Las *Directrices sobre prácticas de IA prohibidas* confirman esta aproximación, al señalar que el concepto de distorsión significativa del comportamiento de la DPCD puede constituir una «válida fuente de inspiración» para interpretar dicho término. Como se ha considerado anteriormente, la cláusula general de deslealtad exige que la práctica comercial tenga la aptitud para distorsionar significativamente el comportamiento económico del consumidor, no exigiendo una distorsión efectiva, si bien el art. 5.1 AIA abarca cualquier tipo de comportamiento —no solo el económico— y toma como referencia a las personas físicas o a colectivos de personas, independientemente de que sean o no consumidores.

Diferencias aparte, de cara a analizar prácticas comerciales personalizadas por IA, la DPCD puede resultar útil para superar ciertas ambigüedades de la AIA. Pese a que las citadas directrices aportan algunos indicios, la AIA no llega a aclarar (ni a lo largo del articulado ni en sus considerandos) qué debe entenderse por una alteración sustancial del comportamiento. La DPCD, en cambio, sí que aporta una caracterización en su art. 2.*e)*, señalando que la distorsión sustancial del comportamiento se equipara a «utilizar una práctica comercial para mermar de manera apreciable la capacidad del consumidor de adoptar una decisión con pleno conocimiento de causa haciendo así que este tome una decisión sobre una transacción que de otro modo no hubiera tomado».

*Mutatis mutandi*s, trasladando esta lógica a las prácticas comerciales manipulativas o subliminales de la AIA, podría entenderse que una alteración sustancial del comportamiento comprende aquellas prácticas llevadas a cabo mediante IA que *a)* tengan como objetivo o efecto mermar de manera apreciable la capacidad del destinatario de tomar una decisión con pleno conocimiento de causa, *b)* haciendo así que este tome una decisión que de otro modo no hubiera tomado.

Ahora bien, si tenemos en cuenta que los otros dos requisitos exigidos por el art. 5.1.*a)* de la AIA son: *a)* la merma apreciable de la capacidad de tomar una decisión informada y *b)* la toma de una decisión que de otro modo no se hubiese tomado, resulta evidente que la prohibición de prácticas manipulativas o subliminales presenta una configuración circular, coincidiendo con la definición de alteración sustancial del comportamiento de la DPCD. En otras palabras, si bien la alteración sustancial del comportamiento en la DPCD era caracterizada por estos dos rasgos, parece que la AIA ha decidido incorporarlos como requisitos expresos e independientes de la alteración sustancial del comportamiento. Ahora bien, al menos en el caso de las prácticas comerciales personalizadas por IA, es evidente que los tres conceptos conforman un único requisito circular, por lo que la aproximación más conveniente pasa por abordarlos de forma conjunta.

4. La merma apreciable de la capacidad de tomar una decisión informada

La merma de la capacidad de toma de decisiones informadas mediante sistemas de IA lleva advirtiéndose como un peligro en el ámbito del derecho del consumo desde hace años. La *Nueva Agenda del Consumidor* de 2020 señaló la necesidad de tomar medidas para hacer frente a prácticas comerciales problemáticas «que ignoran el derecho de los consumidores a elegir con conocimiento de causa, abusan de sus prejuicios de comportamiento o distorsionan sus procesos de toma de decisiones»[87].

Siguiendo criterios similares a la DPCD, la prohibición de técnicas subliminales o manipulativas del art. 5.1.*a)* de la AIA exige que la técnica IA en cuestión merme de manera apreciable la capacidad para tomar una decisión informada. Esta merma se ha analizado previamente desde la óptica de las prácticas desleales agresivas, si bien entendemos que muchos de los argumentos son trasladables a la prohibición de la AIA.

En el caso de los *dark patterns* adictivos, numerosos estudios evidencian cómo el diseño de servicios como las redes sociales y los videojuegos *online* pueden producir un detrimento significativo en las capacidades cognitivas del usuario, llevándole a dedicar un número excesivo de horas a dicho servicio digital e incluso llegando a repercutir negativamente en su salud física y psíquica y su vida *offline*[88]. Estos mismos estudios señalan que los estímulos manipuladores o subliminales producidos por sistemas de IA de caja negra, adaptados y dirigidos

[87] Comisión Europea, *Nueva Agenda del Consumidor…, op. cit.,* 2020.
[88] Cohen, T. «Regulating Manipulative Artificial Intelligence», *op. cit.*

al individuo o a un pequeño grupo en lugar de a la población, son menos susceptibles de ser sometidos al mismo escrutinio público por su alto nivel de personalización y variabilidad[89].

A estos bajos niveles de escrutinio se le suma una ventaja sobre los tradicionales métodos de manipulación comercial: la implacabilidad y resistencia de los sistemas de IA[90]. Los actuales sistemas de IA se basan en modelos de prueba y error que permiten estudiar el comportamiento de un individuo, de forma que sea predecible con altos niveles de eficacia y sin requerir un esfuerzo humano. Se ha señalado así que «la tecnología es inherentemente persistente: un ordenador no se cansa, desanima o frustra como los humanos»[91].

Esta persistencia tecnológica repercute directamente en la merma de la capacidad de tomar decisiones informadas por parte de individuos y colectivos, cuyo proceso de toma de decisiones se ve afectado de forma apreciable por el empleo de estímulos subliminales o manipulativos que se personalizan a través de sistemas de IA conforme al comportamiento *online* de cada usuario.

Otro ejemplo, aparte de los *dark patterns* adictivos, se aprecia en la personalización de precios. Ciertas *apps* de transporte terrestre, como Uber y Cabify, personalizan sus precios de forma manipulativa conforme a una diversidad de información digital sobre el usuario, como su nivel de batería, la localización, la hora, o la gama del dispositivo utilizado para solicitar el servicio de transporte. Un fenómeno similar sucede con el transporte aéreo, en el que el precio de los billetes de avión también se personaliza conforme a una variabilidad de datos, como el interés manifestado por el usuario a través de búsquedas previas[92].

La explotación de datos personales —a menudo reveladores de vulnerabilidades— a través de sistemas de IA para personalizar estas prácticas repercute directamente sobre la capacidad de toma de decisiones. El efecto sobre la formación de la voluntad del usuario se potencia aún más por la falta de alternativas viables que se acomoden a las necesidades o intereses del destinatario[93][94]. Si bien la merma

---

[89] *Ibid.*; Jacobs, N. «Two Ethical Concerns about the Use of Persuasive Technology for Vulnerable People», Bioethics, 34(5), 2020, pp.519-520.

[90] *Ibid.*

[91] *Ibid.*, p. 520.

[92] Murry, C. *et al.* «Price Discrimination in International Airline Markets», *The Review of Economic Studies,* 2019, versión *online*.

[93] Joost, P. y Zuiderveen, B., «Personalised Pricing: The Demise of the Fixed Price?», en Kohl, U. y Eisler, J. (eds.), *Data-Driven Personalisation in Markets, Politics and Law,* Cambridge University Press.

[94] Siguiendo ejemplos anteriores, si todas las *apps* de transporte disponibles en una determinada ciudad personalizan sus precios para ese destinatario concreto en esas circunstancias concretas, el mismo no verá otra opción que aceptar el precio ofertado, por elevado que sea.

apreciable de la capacidad de la toma de decisiones debe apreciarse casuísticamente, no han faltado aportaciones doctrinales que reconocen de forma expresa el carácter deliberadamente manipulativo de ciertas prácticas comerciales llevadas a cabo mediante IA (especialmente, los *dark patterns*)[95].

5. La toma de una decisión que, de otro modo, no se hubiese tomado

El penúltimo requisito exigido por el art. 5.1.*a)* de la AIA para que la práctica IA en cuestión merezca la calificación de prohibida es que haga que una persona o un colectivo de personas «tomen una decisión que de otro modo no habrían tomado». Este requisito se formula como un ilícito de resultado, al exigir la toma de una decisión por parte de una persona o de un colectivo, si bien las únicas decisiones relevantes a efectos de la prohibición son aquellas relacionadas con un perjuicio potencial o efectivo.

La prohibición se articula en este requisito de una forma menos flexible a como se hace en la normativa de prácticas desleales. Desde el plano teórico existen dos formas posibles de configurar la prohibición para considerar la práctica como ilícita bajo un examen de agresividad: *a)* exigir que lleve al consumidor medio a tomar una decisión que de otro modo no hubiera tomado, y *b)* requerir que la práctica comercial *pueda* hacer al consumidor medio tomar una decisión que de otro modo no hubiera tomado[96]. La suficiencia de esta segunda posibilidad ha sido confirmada por la jurisprudencia del TJUE, que advierte que no es necesario que la compra o contratación del servicio se llegue a efectuar[97], argumento que es trasladable igualmente a ciertas prácticas incluidas en la lista negra de prácticas desleales, como el *spam*.

A diferencia de la normativa de prácticas comerciales desleales, la AIA exige la toma efectiva de una decisión por parte de un individuo o por parte de un colectivo como consecuencia de la técnica subliminal o manipulativa llevada a cabo mediante IA. Aunque anteriormente señalábamos que el art. 5.1.*a)* AIA admite la posibilidad de que la práctica no tenga como efecto alterar de manera sustancial el comportamiento, bastando con el objetivo de dicha alteración comportamental, la flexibilidad del precepto se minimiza considerablemente si tenemos en cuenta que la norma exige en la práctica la concurrencia de un resultado, que no es otro que la toma de una decisión que, de no ser por dicha práctica, no se hubiese tomado.

---

[95] Esposito, F. yMaciel Cathoud Ferreira, T. «Addictive design as an unfair…», *op. cit.,*

[96] Art. 8 DPCD y art. 8 (2) LCD.

[97] *Idem*.

Aunque este requisito pueda parecer estricto, no obsta la aplicabilidad de la prohibición en casos que identificábamos como problemáticos. A título de ejemplo, la personalización de precios mediante IA implica la toma de una decisión: contratar o no contratar un servicio. En este sentido, y bajo una interpretación contextual y funcional, se entiende que el término *decisión* incluido en la AIA abarca no solo una opción transaccional en sí misma, sino también las condiciones en las que se ejerce tal decisión. Lo mismo sucede en el caso de los *dark patterns* adictivos. Su personalización adictiva mediante sistemas de IA derivaría también en una decisión viciada: usar compulsivamente un producto o servicio[98]. Como hemos puesto de manifiesto, la capacidad para tomar esta decisión se ve mermada en el caso de los patrones adictivos, precisamente por la explotación y el fomento de la adicción por parte del sistema de IA empleado.

Ahora bien, el art. 5.1.*a)* AIA solo incorpora aquellos riesgos que el legislador comunitario ha marcado como inaceptables, por contravenir los valores de la Unión y el respeto de los derechos fundamentales consagrados en la Carta, como el derecho a la no discriminación y a la protección de datos[99]. Este carácter inaceptable exige que no quede prohibida toda práctica IA manipulativa que afecte el comportamiento, merme la capacidad de toma de decisiones y lleve a tomar una decisión que de otro modo no se hubiese tomado. Se exige, por tanto, un último requisito adicional que define especialmente el carácter inaceptable de la práctica: la provocación o probabilidad de provocación de perjuicios considerables.

6. La provocación o probabilidad de provocación de perjuicios considerables

El último factor que califica a la práctica manipulativa mediante IA como una práctica prohibida es la provocación o la probabilidad de provocación de un perjuicio considerable a la persona afectada por ella, a otra persona o a un colectivo de personas.

Así las cosas, de la formulación del perjuicio exigido por art. 5.1.*a)* AIA se derivan tres extremos: *a)* no es imprescindible la provocación efectiva de un perjuicio, sino que basta con la mera probabilidad de su producción; *b)* el perjuicio —efectivo o potencial— debe ser considerable; y *c)* la persona dañada o potencialmente dañada no tiene por qué ser la persona afectada por la práctica manipulativa, pudiendo ser otra persona o un colectivo de personas.

---

[98] Roffarello, A. y Russis, L. «Towards understanding the dark patterns that steal out attention», *CHI EA '22: Extended abstracts of the 2022 CHI conference on human factors in computing systems,* 2022.

[99] Considerando (28) AIA.

6.1. *La provocación o probabilidad de provocación de un perjuicio*

El considerando 29 del Reglamento confirma que solo es necesaria la probabilidad de que concurra un perjuicio efectivo para que la práctica quede prohibida, sin que sea imperativo que concurra el perjuicio de forma efectiva. Esta probabilidad no debe entenderse como sinónimo de una mera o lejana posibilidad de que la técnica en cuestión derive en un perjuicio, por remota que sea. La RAE define que algo es probable cuando «es bastante posible que ocurra o que sea cierto», y en su acepción matemática, la probabilidad significa «en un proceso aleatorio, razón entre el número de casos favorables y el número de casos posibles». Así las cosas, la probabilidad de que una técnica IA produzca perjuicios implica un examen razonable, excluyendo aquellos casos en los que las posibilidades de que concurra un perjuicio sean escasas, ínfimas o incluso absurdas[100]. En caso de que el daño o perjuicio causado por el sistema de IA se desenvuelva en el marco de una relación contractual, la exigencia de esta probabilidad encuentra conexiones lógicas con las normas generales aplicables a la indemnización por incumplimiento, donde el contratante afectado tiene derecho a que se le indemnicen todos los daños que resulten del incumplimiento y estén causalmente conectados a este, si bien con una excepción importante: no resultan compensables los daños imprevisibles al momento de contratar, siempre que el incumplidor fuera de buena fe[101].

La concurrencia de una probabilidad —que no mera posibilidad— implica el alivio de unas cargas que serían excesivas para el proveedor o responsable del desarrollo, ya que resultaría desproporcionado exigir al mismo que prevea y prevenga todos los posibles perjuicios que un sistema de IA puede causar, por variopintos o inimaginables que resulten. Pese a que este factor moderador beneficia en cierto modo las exigencias aplicables a estos operadores, no debemos pasar por alto que en ningún momento la norma exige una conducta deliberada del proveedor o el responsable de despliegue en la producción del perjuicio real o potencial.

---

[100] A título de ejemplo, un tratamiento de spa que utiliza aromas generados por inteligencia artificial para calmar a los clientes puede afectar al comportamiento de éstos, pero su carácter manipulativo sería ampliamente discutible, así como la probabilidad de que se produzca un perjuicio significativo. Un posible perjuicio podría ser el desarrollo de una alergia al aroma en cuestión, si bien este perjuicio se presenta más como posibilidad escasa que como un suceso probable bajo un cálculo de posibilidades razonables.

[101] Para un análisis más detallado sobre la indemnización por daños en el marco regulatorio español, *vid.* Esplugues García, J. «La infracompensación como excepción al deber de limitar el daño», *Revista Aranzadi de Derecho Patrimonial*, núm. 63, 2024.

En otras palabras, aun en el caso de que el proveedor o responsable no tuviese la intención de causar un perjuicio, la mera concurrencia del perjuicio o su probabilidad de producción implicarían el carácter prohibido de la práctica, asumiendo que se cumplan los demás requisitos del art. 5.1.*a)* AIA ya expuestos[102]. Así lo confirma el considerando 29 de la norma, al señalar que «en cualquier caso, no es necesario que el proveedor o el responsable del despliegue tengan la intención de causar un perjuicio considerable, siempre que dicho perjuicio se derive de las prácticas de manipulación o explotación que posibilita la IA». Así las cosas, la concurrencia o probabilidad de un perjuicio como resultado de la práctica IA conforma un requisito o supuesto objetivo, independiente de la intencionalidad del proveedor o responsable.

6.2. *La magnitud «considerable» del perjuicio y tipos de perjuicios englobados*

Respecto al segundo extremo, la norma exige que el perjuicio —efectivo o probable— sea considerable. Este requisito cumple con un principio de proporcionalidad sobre las cargas exigibles a proveedores y responsables de despliegue, excluyendo del supuesto de hecho a aquellos perjuicios que sean ínfimos, mínimos o irrelevantes, así como a aquellos que no guarden relación con la salud o con los intereses financieros del sujeto o de un colectivo.

La exigencia de un perjuicio considerable, real o probable, cierra filas con la aproximación por riesgo que caracteriza a la AIA, siendo definido el riesgo a efectos del Reglamento como «la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio»[103]. Bajo esta caracterización del riesgo, es lógico y coherente que la prohibición de técnicas manipulativas o subliminales exija la provocación de un perjuicio efectivo o probable de cierta entidad. A efectos prácticos, conviene señalar que las *Directrices sobre prácticas de IA prohibidas* sostienen que no es necesario que el proveedor, el implementador o el sistema que utiliza las técnicas manipulativas tenga la intención de causar perjuicio.

Abordando el requisito de que el perjuicio sea considerable, no obtenemos una definición de tal por la AIA. En cambio, las Directrices sobre prácticas de IA prohibidas sí ofrecen criterios interpretativos para delimitarlo, recalcando que el análisis de estos perjuicios debe realizarse caso por caso. Partiendo de la jurisprudencia del TJUE en casos como el de *Waddenvereniging y Vogelbeschermingsvereniging* o el

[102] Krupiy, T. «Why the Proposed Artificial Intelligence Regulation Does Not Deliver on the Promise to Protect Individuals from Harm», *European Law Blog*, 2022.

[103] Art. 3 *a)*.

de *Sweetman*[104], se hace hincapié en la necesidad de aplicar un enfoque de precaución y protección amplia en la aplicación de la prohibición.

Según las Directrices, el primero de los criterios que se han de tener en cuenta en el análisis es el grado de perjuicio que el uso del sistema de IA pueda causar, teniendo en cuenta efectos objetivos y observables y la posible combinación de distintos tipos de perjuicios que podrían intensificar el perjuicio. A título de ejemplo, siguiendo prácticas que hemos identificado como problemáticas, los patrones oscuros hiperadictivos en redes sociales, plataformas de compra o videojuegos *online* podrían derivar en perjuicios significativos, teniendo en cuenta que pueden producirse perjuicios tanto económicos (compras compulsivas) como en la salud de los usuarios (derivados de la adicción al servicio).

En segundo lugar, se debe tener en cuenta el contexto específico en el que ocurre el perjuicio y los efectos acumulativos de diferentes acciones del sistema de IA. La comparativa con el estado inicial de la persona o grupo afectado, así como la acumulación de impactos, desempeñan un papel crucial en la evaluación de las implicaciones del perjuicio conforme a las Directrices. En tercer lugar, se subraya la importancia de analizar la escala e intensidad del perjuicio, evaluando tanto la extensión del perjuicio como la gravedad de sus efectos adversos. Del mismo modo se deberá tener en cuenta la cantidad de personas afectadas.

En cuarto lugar, se destaca la vulnerabilidad de las personas afectadas, considerando que ciertos grupos, como los menores de edad, las personas mayores o las personas con discapacidad, son más susceptibles a sufrir perjuicios por ciertos sistemas de IA. Las Directrices justifican que un perjuicio que podría parecer menor en términos generales podría ser calificado como significativo cuando afecta a estos colectivos vulnerables. Esta argumentación guarda cierto paralelismo con las alusiones a grupos vulnerables en la DPCD y la LCD, así como en la DSA y la prohibición del art. 5.1.*b)* de la AIA, que prohíbe determinadas técnicas de IA que exploten vulnerabilidades.

Finalmente, se señala que en la evaluación se ha de tener en cuenta la duración e irreversibilidad del perjuicio. Conforme a las Directrices, los perjuicios duraderos o irreversibles tienen más probabilidades de cumplir con el umbral de significación o apreciabilidad del perjuicio, mientras que los efectos temporales o reversibles podrían no considerarse significativos, salvo que sean recurrentes o sistemáticos.

En cuanto a los tipos de perjuicios englobados, los considerandos 28 y 29 de la AIA se refieren *en particular* a perjuicios en la salud

[104] Sentencia del Tribunal de Justicia de 7 de septiembre de 2004, *Waddenvereniging y Vogelbeschermingsvereniging*, asunto C-127/02, EU:C:2004:482, y Sentencia del Tribunal de Justicia de 11 de abril de 2013*, Sweetman y otros*, asunto C-258/11, EU:C:2013:220.

física o mental o en los intereses financieros, que, en ciertos casos, pueden confluir y generar impactos negativos acumulativos y multifacéticos, afectando también al tejido social y contraviniendo los valores fundamentales de la Unión, tales como la dignidad humana, la libertad, la democracia y el Estado de derecho. De esta formulación se desprende que es una enumeración ejemplificativa, si bien las *Directrices sobre sistemas de IA prohibidos* se detienen a ofrecer ciertas notas aclaratorias sobre estos tipos de perjuicios[105].

En primer lugar, las Directrices se refieren al perjuicio físico, que comprende cualquier lesión o perjuicio a la vida o la salud de una persona, así como el perjuicio material a los bienes. Las Directrices subrayan que estos perjuicios son especialmente graves, por cuanto suelen tener consecuencias inmediatas, serias e irreversibles. En coherencia con la lógica de seguridad de los productos, la AIA prohíbe expresamente el uso de sistemas de IA que, mediante técnicas manipulativas o engañosas, sean susceptibles de causar un perjuicio físico significativo. A modo de ejemplo, se mencionan los *chatbots* que incitan a los usuarios a autolesionarse, cometer suicidio o ejercer violencia contra otras personas o colectivos, incluidas minorías, a través de la promoción de contenidos terroristas o discursos de odio.

Las Directrices hacen referencia en segundo lugar al perjuicio psicológico. Éste tiene especial relevancia en los casos de sistemas de IA que explotan vulnerabilidades cognitivas y emocionales para influir en el comportamiento de los usuarios. Entre los perjuicios psicológicos se incluyen efectos negativos sobre la salud mental y el bienestar emocional, los cuales pueden acumularse a lo largo del tiempo y no siempre resultan evidentes de manera inmediata. Las consecuencias pueden ser duraderas y graves, y su evaluación debe realizarse caso por caso. Como ejemplo se señala el uso de aplicaciones de IA que simulan interacciones humanas para fomentar la dependencia emocional y comportamientos adictivos. A nuestro entender, este tipo de perjuicio es de particular relevancia para analizar los patrones oscuros hiper-adictivos, que pueden causar una adicción importante en los usuarios de servicios como los videojuegos *online* o las redes sociales, donde el prestador del servicio tiene varios alicientes económicos para fomentar dicha adicción. Entre ellos, se han señalado previamente los ingresos publicitarios, las compras dentro del mismo servicio, o los propios datos comportamentales del usuario, de un gran valor económico.

Por último, las Directrices sobre prácticas de IA prohibidas destacan los perjuicios financieros y económicos, que abarcan desde pérdidas económicas directas hasta la exclusión financiera o la inestabilidad económica. Ilustran este perjuicio con el caso de *chatbots* que promocionan

---

[105] Whittle, M. *et al., Study to support the Fitness Check of EU…, op. cit.,* pp. 18-28.

productos fraudulentos, causando perjuicios económicos significativos a los usuarios. Entendemos que este perjuicio abarcaría ejemplos expuestos a lo largo del presente trabajo, como la aceptación de un precio personalizado más elevado en situaciones de vulnerabilidad o la compra excesiva de productos por adicción al servicio en el que son ofertados. Las Directrices insisten en que estos perjuicios rara vez se presentan de forma aislada. La combinación de perjuicios físicos, psicológicos y económicos puede agravar el impacto general sobre las personas y las comunidades, e, incluso, producir consecuencias sociales más graves que atenten contra los valores esenciales de la Unión.

Si bien la norma no aborda de forma directa el fomento o la producción de adicciones mediante prácticas de IA (a través de *hiper-engaging dark patterns*), se entiende que la adicción es uno de los perjuicios cubiertos por la norma, al abordar específicamente los daños «con efectos adversos suficientemente importantes en la salud física o mental o en los intereses financieros»[106]. En este punto, el art. 5.1 de la AIA puede resultar particularmente útil para abordar *dark patterns* adictivos que no sean incorporados en plataformas en línea, escapando del ámbito de aplicación personal de la DSA, como sucede con los videojuegos *online*.

Ahora bien, se entiende que la adicción al servicio causada o fomentada por los sistemas de IA debe ser mínimamente importante para que merezca un reproche de ilicitud, causando la calificación de la práctica IA como prohibida. Para considerar la adicción como un perjuicio considerable producido por un sistema de IA, puede resultar útil que la Organización Mundial de la Salud (OMS) decidiese incorporar el denominado «trastorno por uso de videojuegos» o *gaming disorder* en la edición de la Clasificación Internacional de Enfermedades en 2018, bajo la entidad padre de «trastornos debidos a comportamientos adictivos»[107]. La OMS indica que el trastorno por uso de videojuegos se caracteriza por un patrón de comportamiento de juego persistente o recurrente que se manifiesta por: 1) deterioro en el control sobre el juego (por ejemplo, inicio, frecuencia, intensidad, duración, terminación, contexto); 2) incremento en la prioridad dada al juego al grado de que se antepone a otros intereses y actividades de la vida diaria; y 3) continuación o incremento del juego a pesar de que tenga consecuencias negativas.

En el caso de la personalización adictiva de videojuegos a través de sistemas de IA, se podría explotar la adicción causada estudiando comportamientos del usuario en el videojuego concreto o, incluso, analizando globalmente información relativa al usuario en ese servicio

[106] Considerando 29 AIA.

[107] OMS. CIE-11. *Clasificación Internacional de Enfermedades, 11.a revisión. Estandarización mundial de la información de diagnóstico en el ámbito de la salud.*

y en otros, en caso de que el sistema tenga acceso a datos de terceros. Si de la información procesada se deriva una intensidad y una duración excesivas en el uso del servicio o patrones que revelen tendencias a un uso excesivo, podría sostenerse que el sistema de IA provoca (o es probable que provoque) perjuicios considerables en la salud mental del usuario, dando lugar a la calificación de la práctica como prohibida.

En el caso del aumento personalizado de precios en *apps* como Uber, la alteración de este parámetro a partir de vulnerabilidades de los usuarios (manifestadas a través de datos como la localización y la hora) puede tener cabida en el concepto de perjuicio de la AIA, en vista de que el considerando 29 de la norma hace referencia expresa a perjuicios con efectos adversos suficientemente importantes en la salud física o mental *o en los intereses financieros*[108].

Ahora bien, la exigencia de que el perjuicio en los intereses financieros del usuario sea importante puede generar ulteriores problemas. A título de ejemplo, el aumento irrisorio de unos céntimos en el precio personalizado del servicio puede no conllevar un perjuicio considerable para el sujeto afectado, si bien es cuestionable dónde debe trazarse la línea entre un aumento considerable del precio y otro que no lo sea. Tal vez, en este sentido, las vías previstas por la DPCD y su normativa de transposición pueden resultar más adecuadas, en caso de que concurran los requisitos para la agresividad ilícita de la práctica desde la perspectiva del consumidor medio, moderándose esta perspectiva conforme a las circunstancias que rodeen al caso concreto.

6.3. *El sujeto perjudicado por la práctica manipulativa o subliminal: la persona afectada, otra persona o un colectivo*

El tercer extremo que configura este último requisito (el perjuicio real o efectivo causado por la práctica manipulativa o subliminal) es la posibilidad de que la persona dañada o potencialmente dañada no sea la persona afectada por la práctica. El supuesto de hecho del art. 5.1.*a)* AIA prevé que el sujeto dañado sea *a)* el sujeto o colectivo manipulado, *b)* otra persona o *c)* un colectivo de personas. En todo caso, ha de entenderse que puede dañarse de forma cumulativa a varios o a todos los anteriores.

Es destacable que el art. 5.1.*a)* AIA abre la posibilidad de tomar como referencia a una persona individualmente afectada por la práctica, lo que —a diferencia de la DPCD— excluye la necesidad de que la misma sea un consumidor razonablemente informado, atento y perspicaz (coincidiendo con la actual definición del consumidor medio).

---

[108] Considerando 29 AIA, énfasis añadido.

En otras palabras, una de las principales ventajas de la prohibición de técnicas manipulativas o subliminales en la AIA es la posibilidad de examinar las circunstancias concretas del individuo afectado, que puede presentarse como predeciblemente irracional o vulnerable debido a diversos factores, como el diseño adictivo del servicio o las circunstancias que le rodean al aceptar el incremento personalizado del precio.

Por otro lado, si bien la inclusión de los sujetos indirectamente damnificados obedece de forma particular a la tutela de decisiones individuales que afecten a intereses públicos (como las decisiones electorales tras el caso *Cambridge Analytica*), conviene no ignorar que las prácticas comerciales aquí analizadas también presentan la potencialidad de afectar a terceros o a colectivos de consumidores como «víctimas indirectas» de la explotación y análisis comercial de datos.

Recordemos así que la personalización de prácticas IA manipulativas o subliminales es facilitada por el análisis masivo de datos (*Big Data Analytics*), lo que significa que la explotación de datos personales de un sujeto puede perjudicar no solo a los intereses de ese sujeto, sino también a los intereses de terceros o de colectivos[109]. En otras palabras, este doble impacto —individual y colectivo— sucede porque la acumulación y análisis masivo de datos permiten la mejora de las capacidades de deducción y predicción de los sistemas de IA, dando lugar a prácticas comerciales mucho más personalizadas, eficientes e intrusivas en la autonomía de los destinatarios. A título de ejemplo, el análisis de datos personales del usuario de un videojuego contribuye a predecir no solo las reacciones y futuros intereses o necesidades de este, sino también las de otros usuarios con un comportamiento similar, contribuyendo de forma global a que el sistema de IA incremente el diseño adictivo del servicio.

Siguiendo este hilo, algunos autores han comenzado a acuñar el denominado «derecho a un medio ambiente digital saludable», antónimo del término «medio ambiente digital contaminado»[110]. Con esta idea se advierte que el uso de datos personales como contraprestación contribuye a la contaminación del entorno digital al posibilitar la recolección y el análisis de dicha información[111]. El pago con datos generaría, conforme a estos mismos autores, un ambiente digital marcado por la hipervigilancia masiva y personalizada que incide en derechos previamente reconocidos, como el derecho a la intimidad y a la protección

---

[109] Candrian, C., Scherer, A., «Rise of the machines: Delegating decisions to autonomous AI» *Computers in Human Behavior,* vol. 134, 2022.

[110] Zuboff, S. *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder.* Paidós, 2020; y Castillo Parrilla, J.A. «Privacidad de grupo…», *op. cit.*

[111] Castillo Parrilla, J.A. «Privacidad de grupo…, *op. cit.*

de datos o, incluso, en lo que aquí nos atañe, en el derecho a la no discriminación. Se argumenta así que la contaminación del medio digital perjudica no solo a los intereses del destinatario concreto de la práctica, sino también a los intereses de terceros o, incluso, al colectivo general de los consumidores y usuarios. Esta aproximación, a nuestro entender, debe entenderse con cautela y solo debe integrarse en las prohibiciones de la AIA cuando el efecto perjudicial sea claramente significativo para intereses individuales y colectivos.

Contrario sensu, se manifiesta el fenómeno opuesto: la práctica IA manipulativa puede resultar perjudicial para un destinatario concreto, pero puede ser beneficiosa indirectamente para terceros o el común de los consumidores y usuarios, quienes serían no víctimas, sino «beneficiarios» indirectos del perjuicio del primero. En términos económicos, de la práctica IA derivaría una externalidad social positiva. Este caso, desde un punto de vista de política normativa, plantea muchas más disyuntivas, ya que exige encontrar un equilibrio entre los intereses individuales y los intereses colectivos, siendo los contornos de división entre las prácticas IA aceptables e inaceptables todavía más difusos. Pasando a ejemplos prácticos, es posible que la personalización de precios mediante IA perjudique económicamente a un destinatario concreto debido a sus características particulares. Al mismo tiempo, es posible que esta práctica manifieste efectos globalmente positivos sobre el conjunto de los consumidores, ya que diversos estudios sugieren que la personalización de precios también puede incrementar la competencia y fomentar la innovación, ofreciendo nuevas alternativas a los consumidores[112].

En estos casos, para determinar si la práctica IA debe guardar o no la consideración de prohibida, proponemos que se preste una particular atención a los datos que desencadenen la elevación personalizada del precio. A título de ejemplo, la normativa de consumo de la UE no prohíbe de forma absoluta la personalización o discriminación de precios, si bien el art. 16.1 de nuestra LCD reputa como desleal la discriminación de precios *injustificada*[113]. El análisis conjunto de la norma con las prohibiciones de la AIA puede resultar útil para determinar si prácticas como la discriminación de precios mediante sistemas de IA son justificadas y, en consecuencia, conductas desleales.

---

[112] *Vid.* Joost, P. y Zuiderveen, B., «Personalised Pricing…», *op. cit.*; Bourreau, M. *et al.* «Big Data and Competition Policy: Market power, personalised pricing and advertising», *SSRN Electronic Journal*, 2019.; Geradin, D. y Petit, N., «Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles, 2015», *Global Competition Law Centre Working Paper Series*, núm. 07/05; De Streel, A. y Jacques, F. «Personalised pricing and EU law», *30th European Conference of the International Telecommunications Society* (ITS*): «Towards a Connected and Automated Society»,* 2019; y Sears, A. M. «The Limits of Online Price Discrimination in Europe». *Science and Technology Law Review*, *21*(1), 2021, pp. 1-42.

[113] Art. 16 (1) LCD.

Dicho de otra forma, una interpretación sistemática de las prácticas IA prohibidas nos ha de llevar a defender que un aumento personalizado del precio del servicio basado en el procesamiento mediante IA de datos concretos del individuo ha de ser un elemento determinante en la prohibición de la conducta. Y ello con independencia de que la personalización o discriminación de precios pueda repercutir positivamente en el interés colectivo de los consumidores.

A título de ejemplo, no merece el mismo reproche jurídico un incremento del precio del servicio desencadenado a partir del procesamiento de datos que manifiesten una capacidad económica elevada (como el uso de un dispositivo de alta gama), que la aplicación de un precio mayor a partir de la identificación de vulnerabilidades del sujeto utilizando sistemas de IA (como pedir un coche a altas horas de la noche en un barrio inseguro). Aunque ni la personalización ni la discriminación de precios deban ser prácticas reputadas ilícitas *per se* por las posibles ventajas que puede derivar para la competitividad de los mercados, entendemos que las nuevas prohibiciones establecidas por la AIA trazan una línea que exige la apreciación de excepciones, en concreto cuando los sistemas de IA personalicen los precios conforme a vulnerabilidades del destinatario, causando perjuicios considerables en los mismos.

Si bien hasta ahora hemos centrado nuestras reflexiones en las prácticas IA manipulativas o subliminales, el art. 5.1.*b)* de la AIA prohíbe también determinadas conductas basadas en la explotación de vulnerabilidades. Se trata de una prohibición que conecta con la anterior a través de un vínculo de alternatividad o complementariedad. Pasamos a analizar esta prohibición en el siguiente epígrafe.

III. PRÁCTICAS COMERCIALES EXPLOTADORAS DE VULNERABILIDADES

1. El concepto de vulnerabilidad

El concepto de vulnerabilidad ha evolucionado considerablemente en el derecho de la UE, reflejando un enfoque más inclusivo y comprensivo sobre los derechos de los individuos, especialmente en contextos que implican desigualdad de poder, acceso a derechos fundamentales y protección frente a daños. Este concepto ha sido moldeado por diversas normas y directivas que buscan garantizar la protección de los grupos más expuestos y, en consecuencia, la promoción de la dignidad humana, la igualdad y la no discriminación en el marco de la integración europea[114].

[114] Benavides Velasco, P. «Los sujetos (III): consumidores y usuarios ante el reto de la economía colaborativa», en Gosálbez Pequeño, H. (dir.), *Régimen jurídico del consumo cola-*

En un primer momento, el concepto de vulnerabilidad fue abordado de manera más limitada y explícita en contextos como la protección de los consumidores. La Directiva 93/13/CEE del Consejo, sobre cláusulas abusivas en los contratos celebrados con consumidores, fue uno de los primeros instrumentos normativos que reconoció la vulnerabilidad de los consumidores como un factor que podía justificar la intervención del derecho para protegerlos frente a condiciones desproporcionadas o desiguales de negociación. Esta noción de vulnerabilidad, inserta en la DPCD e inicialmente vinculada a la capacidad de las personas para proteger sus derechos e intereses frente a prácticas empresariales, ha evolucionado hacia una protección más amplia en diferentes áreas del derecho de la UE.

De este modo, la normativa y la jurisprudencia han ido incorporando instrumentos de protección ante situaciones de vulnerabilidad en diversos ámbitos. En el marco del derecho social europeo, la jurisprudencia del TJUE ha consolidado una noción más amplia de la vulnerabilidad, considerándola no solo como un factor relacionado con la debilidad económica o contractual, sino también como un atributo que afecta a colectivos sociales específicos. En el art. 8 del RGPD, se subraya la especial protección de los menores al tratar sus datos, considerando que son más vulnerables al uso indebido de su información personal. La vulnerabilidad se vincula ya no solo a un estado de dependencia o debilidad, sino también a la exposición a riesgos derivados del uso de tecnologías.

Así las cosas, el concepto de vulnerabilidad en el derecho de la Unión Europea ha evolucionado desde su aplicación en contextos limitados, como la protección del consumidor, hacia una interpretación más expansiva que abarca cuestiones laborales, tecnológicas y de privacidad. Esta evolución refleja un compromiso de la UE con la protección de los derechos fundamentales, adaptándose a los desafíos contemporáneos en el marco de una sociedad cada vez más interconectada y dependiente de tecnologías avanzadas. La vulnerabilidad, por tanto, se ha convertido en un principio rector para la elaboración de políticas públicas que garanticen la protección de los individuos frente a los riesgos inherentes a la globalización, la digitalización y las desigualdades estructurales en diversas áreas del derecho [115].

En los últimos años, la vulnerabilidad ha sido incorporada al debate sobre la IA y las tecnologías emergentes, especialmente en el contexto

---

borativo, 2019, pp. 163-183; Paniagua Zurera, M. y Miranda Serrano, L. M. «La protección de los consumidores y usuarios y la irrupción del derecho de los consumidores», en Miranda Serrano, L. M.; Pagador López, J. (coords.), *Derecho (privado) de los consumidores*, 2012, pp. 19-62.

[115] Diéguez Aguilera, L. «El consumidor vulnerable: en especial, la vulnerabilidad de las personas mayores ante la acusada digitalización del mercado financiero», *Diario La Ley,* 2023.

de los sistemas automatizados que pueden manipular el comportamiento de los usuarios. En este sentido, la Comisión Europea ha manifestado preocupación por los riesgos de vulnerabilidad asociados al uso de sistemas de IA que explotan las emociones y las decisiones autónomas de los individuos. En su *Comunicación sobre la Inteligencia Artificial*, la Comisión ya advertía que los individuos pueden estar expuestos a riesgos sustanciales cuando interactúan con sistemas que manipulan sus elecciones o comportamientos, identificando a los grupos más vulnerables, como los menores o los usuarios con discapacidades cognitivas.

Estas preocupaciones resultaron en la inserción de una prohibición específica en el art. 5.1.*b)* de la AIA. Una lectura conjunta de las prácticas IA manipulativas o subliminales y las prácticas que exploten vulnerabilidades evidencia que es probable que algunas de las conductas anteriormente analizadas puedan subsumirse en varias de estas prohibiciones. Conviene aclarar, igualmente, que las Directrices sobre prácticas de IA prohibidas advierten, a efectos sancionadores, que esta acumulación debe respetar el *principio ne bis in idem*. En consecuencia, las sanciones no pueden ser acumulativas cuando la práctica de IA contravenga dos o más prohibiciones. No obstante, resulta necesario analizar la inclusión de las prácticas anteriormente consideradas como situaciones de explotación de vulnerabilidades mediante sistemas de IA.

2. Similitudes y diferencias reseñables con respecto a las prácticas de IA manipulativas o subliminales

A raíz de las crecientes preocupaciones sobre el uso de sistemas de IA para explotar de forma perjudicial las vulnerabilidades de los individuos, el art. 5.1.*b)* prohíbe «la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra».

En otras palabras, la prohibición exige la concurrencia de los siguientes requisitos sobre el sistema de IA: *a)* la actividad comprendida es la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA; *b)* debe explotar vulnerabilidades de las personas derivadas de su edad, discapacidad o situación socioeconómica; *c)* dicha explotación debe tener como objetivo o efecto alterar de manera

sustancial el comportamiento de la persona o colectivo afectado y *d)* la alteración del comportamiento debe causar, o ser razonablemente probable que cause, un perjuicio significativo, ya sea a la persona directamente afectada o a otro individuo o colectivo.

A todas luces, la configuración de esta prohibición comparte una amplia base común con la prohibición de técnicas manipulativas o subliminales. Los requisitos *a)* y *c)* a *d)* anteriormente señalados se encuentran, de forma idéntica, en la prohibición de prácticas manipulativas, subliminales o engañosas del art. 5.1.*a)* AIA. A esto se suman no solo las similitudes en sus requisitos, sino la racionalidad misma de las prohibiciones que, como confirman las *Directrices sobre prácticas de IA prohibidas*, no es otra que proteger a los individuos frente a la explotación de sus vulnerabilidades. Entendemos que a causa de este motivo las Directrices analizan todas estas prohibiciones bajo la misma sección, diferenciando únicamente el análisis en el foco de la acción prohibida. Esto es, mientras que en el apartado *a)* del art. 5.1 de la AIA el foco de la acción prohibida se sitúa en la manipulación, la subliminalidad o el engaño; el apartado *b)* se centra en la explotación de determinadas vulnerabilidades.

A efectos de evitar reiteraciones innecesarias, daremos por reproducidos los requisitos idénticos ya analizados con ocasión de las prácticas manipulativas o subliminales[116]. Así las cosas, nos centraremos en estudiar en el siguiente epígrafe el núcleo de la práctica de IA prohibida, a saber, la explotación de vulnerabilidades de las personas derivadas de su edad, discapacidad o situación socioeconómica, aplicado a prácticas comerciales personalizadas mediante sistemas de IA.

3. La explotación de vulnerabilidades a través de sistemas de IA

El eje de la prohibición del art. 5.1.*b)* de la AIA se cimienta sobre la explotación de vulnerabilidades a través de sistemas de IA. El propio término «explotación» revela ya una connotación negativa, en consonancia con la naturaleza del precepto, que no es otra que una prohibición absoluta sobre un riesgo que el legislador de la UE presume como inaceptable. En este sentido, la RAE define la explotación como

[116] Con estos requisitos idénticos nos referimos a: *a)* la introducción en el mercado, la puesta en servicio o la utilización del sistema de IA, *b)* el objetivo o efecto de la práctica, que es la alteración sustancial del comportamiento de una persona o un colectivo de personas, y *c)* la provocación o probabilidad de provocación de perjuicios considerables. Debe notarse, por otro lado, que la prohibición de técnicas explotadoras de vulnerabilidades (a diferencia de aquella que opera sobre las técnicas manipulativas o subliminales) no exige los siguientes requisitos: *a)* una merma apreciable de la capacidad de tomar una decisión informada, ni *b)* provocar la toma de una decisión que de otro modo no se hubiese tomado.

el «conjunto de elementos e instalaciones dedicados a sacar provecho de una fuente de riqueza o de un recurso» y la acción de explotar (en su segunda acepción) como «sacar utilidad de un negocio o industria en provecho propio».

En lo que atañe a este estudio (la explotación de vulnerabilidades para la personalización de prácticas comerciales *online*) ambas definiciones resultan sumamente oportunas. Ambas nociones ponen de manifiesto un claro interés económico. Siguiendo nociones anteriores, los sistemas de IA que personalizan prácticas comerciales *online* tratan de obtener el rendimiento de una situación ventajosa, la vulnerabilidad del sujeto, y utilizan la misma para obtener un provecho económico y/o competitivo en relación con diversos operadores del mercado (el propio prestador del servicio o un tercero al que transmite los datos reveladores de dicha vulnerabilidad).

En el contexto de la discriminación de precios, la explotación se manifiesta en la utilización de información que revela condiciones particulares de los consumidores, tales como su capacidad económica percibida, su nivel de urgencia o su desconocimiento del funcionamiento del mercado. Utilizando complejos sistemas de IA, las empresas identifican y categorizan a los consumidores según su predisposición a pagar un precio más elevado, fijando tarifas personalizadas que no reflejan un criterio objetivo de determinación del precio, sino una evaluación de la debilidad o fortaleza económica del individuo. Esta estrategia se basa en la explotación de la asimetría informativa entre el proveedor y el consumidor, quien desconoce tanto la existencia de un tratamiento diferenciado como los parámetros utilizados para establecer dicho precio. En consecuencia, se reduce de manera significativa su capacidad de comparación y negociación, afectando su libertad contractual.

Un ejemplo de explotación de vulnerabilidades en la personalización o segmentación de precios sería Uber. Un estudio español mostró que las compañías Uber, Cabify y Bolt tienden a fijar precios más altos en barrios con rentas inferiores, al tener menos demanda[117]. Otros estudios revelan que Uber tiende a elevar los precios a aquellos usuarios con baja batería en el móvil[118].

En el caso del fomento de compras compulsivas, la explotación de vulnerabilidades reside en la identificación y manipulación de sesgos cognitivos ampliamente estudiados en la psicología del comportamiento, tales como la aversión a la pérdida, el sesgo de escasez o el efecto de inmediatez. Las prácticas comerciales que inducen a compras impulsivas utilizan estos mecanismos para activar respuestas emocionales

[117] Observatorio de Trabajo, Algoritmo y Sociedad, «Adversarial Audit of ride-hailing…», *op. cit.*

[118] The Brussels Time, «Uber fares allegedly linked…», *op. cit.*

automáticas que anulan o dificultan el juicio racional. La presión para tomar decisiones inmediatas, sin posibilidad de reflexión o consulta, se fundamenta en la explotación de la ansiedad o el miedo a perder una oportunidad, debilitando la autonomía del consumidor. Esta explotación es más intensa en aquellos individuos que presentan dificultades para procesar información compleja o que tienen menor experiencia en el entorno digital, lo que agrava su situación de desventaja frente al operador comercial.

En cuanto al fomento de adicciones en redes sociales y videojuegos, advertíamos que la explotación se centra en la vulnerabilidad psicológica inherente a los sistemas de recompensa del cerebro humano. Las plataformas digitales desarrollan entornos diseñados específicamente para maximizar la liberación de dopamina a través de estímulos constantes y recompensas intermitentes, aprovechándose de la propensión natural del individuo a la búsqueda de gratificación inmediata. Esta manipulación resulta particularmente eficaz en personas con una mayor predisposición a desarrollar conductas adictivas, como los menores de edad o quienes presentan condiciones de salud mental preexistentes. La prolongación artificial del tiempo de conexión y la generación de dependencia funcional refuerzan la posición de control del operador sobre el usuario, quien queda atrapado en un ciclo de comportamiento compulsivo difícil de interrumpir de manera voluntaria.

Acudiendo a un último ejemplo, la personalización de anuncios comerciales explota vulnerabilidades emocionales y psicológicas, mediante la segmentación precisa de los consumidores a partir de datos íntimos o contextuales que revelan estados de necesidad, inseguridad o deseo. Los mensajes publicitarios se diseñan no solo para informar, sino para influir en los estados emocionales del receptor, dirigiéndose a sus miedos, aspiraciones o carencias específicas. Esta explotación se agrava cuando se dirigen contenidos a individuos en situaciones personales sensibles, como problemas económicos, soledad o enfermedades, incrementando la probabilidad de que adopten decisiones de consumo que no responderían a un análisis racional o a un interés auténtico. Así, se produce una manipulación de la voluntad que puede desdibujar el consentimiento informado y libre, fundamento esencial de cualquier relación jurídica contractual.

En todas estas prácticas, la explotación de las vulnerabilidades del consumidor no es incidental, sino deliberada, planificada y sistemática, y responde a un modelo de negocio basado en la maximización del control sobre las decisiones de los individuos y en la explotación de vulnerabilidades. Ahora bien, aunque el concepto de vulnerabilidad se plantea tradicionalmente como generalmente amplio, conviene estudiar, a efectos de la prohibición del art. 5.1.*b)* de la AIA, si las causas

de vulnerabilidad previstas por la norma conforman una lista abierta o cerrada, y quiénes pueden ser los sujetos afectados por dicha explotación.

4. Concreción de los sujetos pasivos: causas de vulnerabilidad del art. 5.1.*b)* AIA y prácticas prohibidas combinadas

Antes de analizar las causas de vulnerabilidad que caen en el ámbito de la prohibición de explotar vulnerabilidades, hemos de detenernos a precisar quiénes son los sujetos pasivos de la prohibición. Como indican las *Directrices sobre prácticas de IA prohibidas*[119] y se ha considerado en secciones anteriores, los sujetos obligados por las prohibiciones del art. 5 AIA (sujetos activos) son los proveedores y responsables de despliegue.

Volviendo a los sujetos pasivos, conviene aclarar que el sujeto afectado por la explotación de vulnerabilidades no tiene por qué coincidir necesariamente con el sujeto perjudicado. Es decir, la literalidad del precepto distingue entre la explotación de vulnerabilidades «de una persona física o un determinado colectivo de personas», —que serían los sujetos afectados por el núcleo de la prohibición y los sujetos perjudicados por dicha práctica prohibida— y la posibilidad de que la misma «provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona *o a otra*» (énfasis añadido). Por tanto, es posible que una práctica de IA explote las vulnerabilidades de una persona física y que esta actividad derive en daños a un tercero. A modo de ejemplo, las *Directrices sobre prácticas de IA prohibidas* citan los *chatbots* que incitan a la violencia contra otras personas o colectivos, incluidas minorías, a través de la promoción de contenidos terroristas o discursos de odio.

Pasando a los sujetos afectados por la explotación de vulnerabilidades, el precepto hace alusión a «vulnerabilidades de una persona física o un determinado colectivo de personas», por lo que se entiende que el mismo contempla dos alternativas.

La primera es la explotación de vulnerabilidades de una persona física por lo que, convenientemente, la prohibición abarcaría aquellas prácticas comerciales altamente personalizadas conforme a las características individuales de cada destinatario. Se acogerían así, a título de ejemplo, la personalización de precios y de anuncios o el fomento de adicciones a servicios como las redes sociales y los videojuegos *online* a través de su diseño (*hyper-engaging dark patterns*). Esta inclusión resulta conveniente, teniendo en cuenta que, en el examen de prácticas comerciales desleales, planteábamos la problemática de identificar

[119] European Commission, *Communication to the Commission. Approval of the content of the draft…, op. cit.,* p. 10.

al miembro medio de un grupo de consumidores vulnerables, cuando dicho grupo no es claramente identificable debido al alto grado de individualización de la práctica.

La segunda alternativa es la explotación de vulnerabilidades de un determinado colectivo de personas, lo que incluiría prácticas como la segmentación de precios, la presentación de publicidad o el desarrollo de otras prácticas comerciales basadas en perfiles grupales. Esta alternativa requiere, al igual que en la problemática que planteábamos anteriormente, la identificación de un grupo de referencia, por lo que se reafirma el carácter conveniente de que el legislador decidiese incluir también como alternativa de sujeto afectado a una persona física individualmente considerada.

Respecto a las causas de vulnerabilidad contempladas, la redacción del art. 5.1.*b)* de la AIA puede resultar un tanto confusa. En un primer momento, el precepto hace referencia a «alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas». El uso del término «alguna» (en su versión original inglesa, *any of the vulnerabilities)* puede dar a entender que cualquier causa de vulnerabilidad queda acogida en el precepto, lo cual dotaría a la norma de una gran elasticidad (como es el caso de la vulnerabilidad en la DPCD). Esta ventaja también puede contemplarse como un riesgo de inseguridad jurídica. Ahora bien, si se continúa leyendo, el precepto hace alusión a vulnerabilidades «derivadas de su edad o discapacidad, o de una situación social o económica específica». La contraposición de estos encajes hace entonces dudar de si nos encontramos ante un *numerus apertus* o un *numerus clausus* de causas de vulnerabilidad. El considerando 29 de la norma tampoco aporta una clave definitiva, puesto que se refiere a «vulnerabilidades de una persona o un colectivo específico de personas derivadas de su edad, su discapacidad […] o de una situación social o económica concreta», si bien añade como ejemplos de este último factor «vivir en condiciones de pobreza extrema o pertenecer a minorías étnicas o religiosas».

Algo más de luz aportan las *Directrices sobre prácticas de IA prohibidas*[120], en las que se sostiene que el concepto de vulnerabilidad puede entenderse en un sentido amplio, abarcando un espectro diverso de categorías que incluyen «la vulnerabilidad cognitiva, emocional, física y otras formas de susceptibilidad que puedan afectar la capacidad de una persona física, o de un grupo de personas, para adoptar decisiones informadas o, en su caso, influir en su comportamiento». No obstante, afirman que, si bien el art. 5.1.*b)* de la AIA se refiere a «cualquier» vulnerabilidad, el ámbito subjetivo de aplicación de la

[120] European Commission, *Communication to the Commission. Approval of the content of the draft…», op. cit.,* p. 34.

prohibición se circunscribe a aquellas personas cuya situación esté definida por su edad, discapacidad o situación socioeconómica específica, ya que dichos colectivos se presumen, en principio, dotados de una capacidad más limitada para reconocer o resistir las prácticas manipuladoras o explotadoras derivadas del uso de sistemas de IA, y, por ello, requieren una protección reforzada.

Así las cosas, las Directrices concluyen que dicha situación de vulnerabilidad debe ser consecuencia directa de que la persona física o el grupo de personas pertenezca a alguno de los colectivos allí mencionados. Aclaran, en otras palabras, que la vulnerabilidad debe estar objetivamente vinculada a una característica inherente a la edad, la discapacidad o la situación social o económica concreta de los afectados.

Visto así, el propósito de esta argumentación en las Directrices parece situarse en no limitar de forma excesiva el concepto de vulnerabilidad, dando cabida a una interpretación flexible. Ello a pesar de que, respetando la literalidad de la norma, parezca exigirse que la práctica aproveche o explote de alguna manera la edad, discapacidad, o una situación social o económica específica del sujeto o grupo en cuestión. Así las cosas, queda claro que la norma acoge claramente las prácticas dirigidas a menores y ancianos, cuyas capacidades pueden verse limitadas en ciertas circunstancias o ante determinadas prácticas comerciales o contratos. El mismo argumento sería aplicable a la explotación de vulnerabilidades por discapacidad. La alusión a «una situación social o económica específica» confirma, por otro lado, la voluntad del legislador de formular esta prohibición de una manera flexible, ya que esta causa puede entroncar con muchas prácticas comerciales problemáticas que veníamos identificando, como alzar el precio de transportes a demanda en barrios inseguros y a altas horas de la noche.

Parece lógico afirmar que la prohibición de prácticas explotadoras de vulnerabilidades puede coincidir, en casos concretos, con la prohibición de técnicas manipuladoras o subliminales que analizábamos en apartados anteriores. A esta misma conclusión llegan las *Directrices sobre prácticas de IA prohibidas*[121], subrayando el carácter complementario de ambas prohibiciones, si bien se ocupan de delimitar ciertas diferencias en sus respectivos propósitos.

Por un lado, la prohibición de la letra *a)* del art. 5.1 se centra en la naturaleza de las técnicas empleadas por el sistema de IA, especialmente aquellas que operan por debajo del umbral de la conciencia o que son intencionalmente manipuladoras o engañosas. Dichas prácticas influyen de forma encubierta en el comportamiento de las personas, menoscabando su autonomía cognitiva para tomar decisiones informa-

[121] *Ibid.*, p. 34.

das y libres, sin necesidad de que se vincule esta manipulación a una vulnerabilidad concreta.

Por su parte, la letra *b)* del art. 5.1 AIA se orienta a proteger a aquellas personas especialmente vulnerables debido a su edad, discapacidad o situación socioeconómica específica. En estos casos, el sistema de IA explota vulnerabilidades inherentes a estos colectivos, quienes, por su propia condición, cuentan con una capacidad reducida para reconocer o resistir prácticas manipuladoras. Por ejemplo, mientras que un sistema que utiliza destellos de imágenes rápidas para influir en decisiones de compra podría encuadrarse en la letra *a)* por la naturaleza subliminal de la técnica, un sistema que dirige ofertas de seguros a personas de edad avanzada, aprovechándose de su limitada capacidad cognitiva, se regiría por la letra *b)*.

Las Directrices concluyen que, cuando ambas disposiciones pudieran ser aplicables, el criterio primordial de diferenciación radica en el aspecto dominante de la explotación. Si la manipulación se produce de forma general, sin atender a vulnerabilidades específicas, prevalecerá el enfoque de la letra *a)*, aunque se deberán tener en cuenta los efectos particulares sobre los colectivos vulnerables. Por el contrario, cuando la explotación se oriente de manera dirigida hacia un grupo especialmente vulnerable, la aplicación del art. 5.1.*b)* resulta procedente. En definitiva, las Directrices sostienen que esta interacción busca equilibrar la protección general contra prácticas manipuladoras con una salvaguarda reforzada para aquellos colectivos que, por sus características inherentes, requieren una protección adicional frente a la explotación por parte de los sistemas de IA.

Pese a estas guías generales, entendemos que en casos concretos puede seguir planteándose la duda de si una práctica se encuadra en la letra *a)* o en la letra *b)*, para lo cual será de gran relevancia un seguimiento de la aplicación práctica y progresiva de la AIA. Ahora bien, a efectos sancionadores (que es lo que más interesa desde la perspectiva de la seguridad jurídica empresarial y de la protección de los sujetos afectados), probar la posible concurrencia de ambas prohibiciones no desplegaría efectos sustantivos, como se justificará a continuación.

IV. CONSECUENCIAS DERIVADAS DE LA INFRACCIÓN DE LAS PROHIBICIONES DE LA AIA Y SU CONVIVENCIA CON OTRAS INFRACCIONES PARALELAS BAJO LOS PRINCIPIOS DE PROPORCIONALIDAD Y *NE BIS IN IDEM*

A efectos prácticos, la principal consecuencia jurídica con que se sanciona la introducción en el mercado, la puesta a disposición o la utilización de sistemas de IA que se sirvan de técnicas manipulativas o su-

bliminales prohibidas es la imposición de multas administrativas de hasta 35 000 000 euros o, si el infractor es una empresa, de hasta el 7 por ciento de su volumen de negocios total anual a escala mundial correspondiente al ejercicio anterior, si esta cifra es superior[122]. En caso de que una misma práctica contravenga uno o más preceptos de la AIA, las *Directrices sobre prácticas de IA prohibidas* aclaran que operará el principio *ne bis in idem*, por lo que no se produciría una acumulación de sanciones[123].

Ahora bien, cabe plantearnos si una misma práctica puede acumular las sanciones consideradas por la AIA a otras previstas por otras normas que la conducta pudiera infringir también. El art. 5.8 de la AIA señala que este artículo (referente a las prácticas de IA prohibidas) no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de derecho de la Unión. Por su parte, el considerando 29 indica que la prohibición de tales prácticas de IA *complementa* lo dispuesto en la DPCD, por lo que se entiende que las acciones previstas en la LCD (tratadas anteriormente) y las sanciones derivadas de normas como la AIA son absolutamente compatibles, puesto que no hay identidad de intereses protegidos.

Mayores dudas puede plantear la acumulación de sanciones administrativas por infracción de diversas normas aplicables a una misma conducta. Remitiéndonos a apartados anteriores, es posible que una misma práctica IA basada en perfiles pueda infringir: *a)* la AIA, en caso de que la práctica comercial incumpla alguna de las prohibiciones de su art. 5 AIA, como la prohibición de técnicas subliminales o manipulativas; *b)* el RGPD, por basarse en datos tratados ilícitamente; *c)* la DMA, en el caso de que la práctica se base en una combinación de datos prohibida por el art. 5.2 DMA y se lleve a cabo en un servicio básico de plataforma prestado por un guardián de acceso; y *d)* la DSA, en caso de que la práctica comercial constituya un anuncio basado en la elaboración de perfiles utilizando datos sensibles (art. 26.3 DSA) presentado en una plataforma en línea[124].

Un ejemplo práctico podría ser la presentación en Facebook de un anuncio basado en la elaboración de perfiles utilizando datos sensibles, siendo dichos datos tratados y combinados ilícitamente (por ejemplo, a través de un consentimiento inválido o incumpliendo principios generales del RGPD), concurriendo los requisitos pertinentes para que dicha práctica

---

[122] Art. 99 (3) AIA.

[123] European Commission, *Communication to the Commission. Approval of the content of the draft…, op. cit.,* p. 18.

[124] Como advertíamos en apartados anteriores, a los que nos remitimos, en el caso de los dark patterns el legislador comunitario sí que aporta ciertas normas de prevalencia. En el art. 25 (2) DSA se aclara que cuando un determinado *dark pattern* resulte ilícito conforme a la DPCD y/o al RGPD no operará la prohibición de patrones oscuros del art. 26 (1) DSA.

sea considerada una técnica de IA manipulativa, subliminal o explotadora de vulnerabilidades que contravenga las prohibiciones de la AIA[125].

Aunque dichas infracciones puedan llegar a ser acumulables, desde un punto de vista sancionador surge la duda de cómo operarían los principios de proporcionalidad y *ne bis in idem* en un ejemplo como el mencionado anteriormente. A la hora de enjuiciarlo se ha de tener en cuenta que permitir una acumulación excesiva de sanciones podría llegar a producir un efecto desincentivador (*chilling effect*), pues el exceso de disuasión podría frenar el desarrollo de usos de IA que pudieran estimarse como arriesgados. Siguiendo una interpretación sistemática de la normativa de la UE aplicable y de sus principios inspiradores, parece que la respuesta más razonable pasaría por determinar si tanto los intereses protegidos como la acción relevante sancionada por cada norma son los mismos, o si difieren en cierta medida.

V. VALORACIONES FINALES

La prohibición de técnicas manipulativas o subliminales de la AIA comparte buena parte de su fundamentación con la DPCD, si bien presenta diferencias sustanciales que pueden hacer que su régimen de aplicación manifieste ventajas con respecto a esta última. Entre las más significativas, cabe subrayar la propia naturaleza de cada norma[126]. Pese a que ambas se formulen como normas de armonización máxima, conviene no ignorar que la AIA (como Reglamento de la Unión) evita las divergencias e incoherencias sufridas por la DPCD en su transposición a la normativa de los Estados miembros[127]. Asimismo, la falta de una normativa nacional preexistente evita la necesidad de conciliación o adaptación, suponiendo una mayor seguridad jurídica para los operadores y evitando restricciones al mercado único en la comercialización de sistemas de IA.

La prohibición de prácticas manipulativas o subliminales de la AIA también presenta virtudes con respecto a otros Reglamentos

---

[125] No conviene olvidar que para que concurran dichas infracciones no solo deben cumplirse los requisitos pertinentes del ámbito material de cada norma, sino que también es preciso examinar si el prestador queda amparado por el ámbito personal de cada una de ellas. En este ejemplo, al presentarse el anuncio a través de Facebook, se cumpliría con el ámbito personal de la DSA, al presentarse en una plataforma en línea, así como de la DMA, al basarse en datos combinados entre servicios básicos de plataforma de un guardián de acceso.

[126] Limongelli, R. «Caveat Emptor de AI, from Black Box to Glass Box: Reviewing Consumer Protection against AI-Enabled Manipulation in the European Union», 2023.

[127] En el caso de la Ley de Competencia Desleal española, la transposición de la DPCD se enfrentó a un difícil proceso de conciliación con una regulación de competencia desleal sólida y arraigada, dando lugar a resultados ampliamente criticados por la doctrina. Por todos, *vid.* Tato Plaza, A. Fernández Carballo-Calero, P. y Herrera Petrus, C. *La reforma de la ley de competencia…, op. cit.*

previamente analizados. A diferencia del RGPD, que es excesivamente aséptico con los efectos del tratamiento de datos personales, la AIA es particularmente sensible con los efectos derivados del tratamiento. Otro aspecto positivo es que la prohibición no depende del concepto de datos personales o de datos sensibles, ya que se formula en torno a conceptos más flexibles (las técnicas manipulativas o subliminales). Con respecto a la DSA y la DMA, advertíamos en anteriores ocasiones la excesiva dependencia de estos reglamentos sobre conceptos clásicos de la normativa de protección de datos (como la noción de datos sensibles, o el consentimiento), dependencia que el art. 5.1.*a)* AIA logra evitar. De igual forma, el ámbito personal de este último precepto es mucho más amplio que aquel de la DSA y de la DMA, al no restringirse a los proveedores de servicios de plataforma y a los guardianes de acceso, respectivamente.

En conclusión, si bien la posible acumulación de sanciones, como veníamos exponiendo, debe analizarse con cautela, ha de valorarse positivamente la relación de complementariedad entre las normas anteriormente analizadas y la AIA. Particularmente, se debe valorar la conexión entre normas teniendo en consideración que las prácticas prohibidas analizadas, por su configuración flexible (tanto en el ámbito personal como material) pueden llegar a formularse como vías eficaces para paliar prácticas no abordadas por normativa precedente y que constituyan riesgos inaceptables para el sistema de derechos y valores de la Unión.

CONCLUSIONES

Fruto de la evolución de nuestro propio objeto de estudio, su título ha sufrido no pocos vaivenes. Esta mutabilidad iba en paralelo con su propia naturaleza, actual y novedosa, advertida desde sus inicios como un arma de doble filo. Pese a todo, dicha novedad marca el carácter y el sentido propio del trabajo, entendiendo que intentar dar respuestas jurídicas a entornos cambiantes no es sino un deber social que debe marcar la labor de los académicos dedicados al análisis crítico del derecho.

Así las cosas, la obra ha estado comprometida, desde sus inicios, con una práctica cambiante, que es la personalización en el desarrollo de prácticas comerciales en los mercados digitales y, más concretamente, en relación con la actividad publicitaria. Este compromiso nace de una preocupación constante en la política de la UE de las últimas décadas, centrada en superar los efectos adversos derivados de la actividad de grandes plataformas en el mercado único digital y en nuestro sistema de valores y derechos fundamentales. Los principales focos de atención se han dirigido a la lucha contra la discriminación y a la protección de la autonomía de la voluntad. La propia forma de referirnos a las conductas analizadas, «la explotación», deja entrever, en cierto modo, que el punto central de análisis se proyecta sobre las utilizaciones negativas o adversas de la personalización.

Dicho esto, el trabajo no es ajeno a los usos positivos que puede conllevar la elaboración de perfiles comerciales, entre los que destaca la filtración de contenidos de mayor interés en un ámbito digital marcado por el exceso de información. En suma, esta personalización permite reducir los costes de transacción derivados de encontrar la información o el producto pertinente en un contexto decisorio marcado por la abundancia. Tales efectos positivos son tenidos en cuenta en el

presente examen, si bien el foco se sitúa, como adelantábamos, en sus efectos perjudiciales, particularmente cuando los sujetos afectados presentan características (intrínsecas o circunstanciales) especialmente vulnerables.

Aunque el legislador de la UE se ha esforzado por establecer mecanismos (*ex ante* y *ex post*) para combatir los efectos perniciosos del procesamiento digital de datos para llevar a cabo prácticas personalizadas con potencialidad lesiva, a lo largo del estudio se han evidenciado deficiencias sustanciales en la regulación. Llegamos, incluso, a plantearnos si nos encontramos ante una hiperregulación de papel mojado, dado el amplio espectro de normas aplicables y su limitada virtualidad efectiva. Con ánimo no de resultar pesimistas, sino de reflexionar y optar por vías jurídicas que guarden un efecto útil, concluimos este estudio con las conclusiones que a continuación siguen, todas las cuales podrían haber conformado títulos alternativos del presente trabajo o, al menos, de las secciones que lo componen.

I. LA ASEPSIA DE LAS PROHIBICIONES ABSOLUTAS ANTE LOS EFECTOS POSITIVOS DE LOS PERFILES PUBLICITARIOS QUE UTILIZAN DATOS SENSIBLES

El valor económico de los datos es un hecho que se ha puesto de manifiesto en la última década de forma particular en el mercado de la publicidad digital. Las continuas reivindicaciones a favor de una prohibición de la publicidad *online* personalizada desembocaron en lo que, en su momento, pudo parecer una solución intermedia entre tales exigencias sociales y los intereses económicos de los diversos operadores que participan en la publicidad *online*. Nos referimos a la decisión del legislador de la UE de prohibir, a través de la DSA, a los prestadores de plataformas en línea presentar publicidad basada en perfiles utilizando datos sensibles.

De este modo, la política normativa de la Unión abordaba las crecientes preocupaciones sociales por el auge de la publicidad personalizada, situadas, particularmente, en los riesgos sobre la privacidad, la protección de datos, la no discriminación y la protección de la libre toma de decisiones. El presente estudio ha subrayado las limitaciones del ámbito personal y material de dicha prohibición. Este análisis objetivo precisa sumar una reflexión sobre la racionalidad misma de dicho precepto o, dicho de otra forma, sobre si esta decisión legislativa obedece a unos criterios o principios que tengan sentido en el acervo de la UE.

La respuesta pasa por determinar si el establecimiento de una prohibición absoluta como la referida responde a los principios rectores

de este acervo, entre los que destaca el principio de proporcionalidad, el cual exige un justo equilibrio entre los diversos intereses contrapuestos. Dicho de otra forma, conviene valorar si el camino hacia prohibiciones absolutas en sede publicitaria toma un rumbo que consideremos adecuado. Esta vía no carece de precedentes, habiendo sido precedida por determinadas prohibiciones sobre anuncios de tabaco, alcohol, armas o juegos de azar, en las que el legislador decidió priorizar ciertos intereses públicos (como la salud o la seguridad) sobre la libre actuación en el mercado de los operadores afectados.

Ahora bien, en el caso de la publicidad basada en perfiles utilizando datos sensibles, este equilibrio de intereses se dificulta. Los intereses económicos se mantienen, toda vez que, en el otro lado, permanece la protección de los intereses y derechos de los destinatarios (como la privacidad o la no discriminación). Resulta fundamental subrayar que dichos derechos no se ven perjudicados siempre y automáticamente por todo anuncio basado en datos sensibles. Es más, el propio anuncio puede presentarse como beneficioso o útil para el destinatario, sirviendo para filtrar información que le sea de interés.

El problema de origen aquí detectado es la creciente tendencia del legislador de la UE a realizar una aproximación basándose en la naturaleza de los datos y no en los efectos o usos particulares de los mismos. Esta tendencia es un legado de la normativa de protección de datos, por la cual todo tratamiento que contravenga sus principios y preceptos se traduce en un reproche de ilicitud, sin resultar relevante si el tratamiento de tales datos ha derivado o no en daños (aunque su concurrencia guarde importancia a efectos sancionadores y compensatorios).

En suma, la creciente asepsia de la normativa de la UE con respecto a los usos positivos de los datos personales, así como la minimización de otros intereses (como la libertad de empresa, o el fomento de la competencia) obligan a replantear si la vía de las prohibiciones absolutas se plantea como una vía justa y proporcionada para la política legislativa. En otras palabras, la vía de las prohibiciones absolutas debe ser un camino a tomar con cautela en la futura política normativa. Se plantea la conveniencia de dotar de un mayor protagonismo a los efectos (probables o reales) del tratamiento de datos personales, y no a su naturaleza, adoptando una verdadera aproximación por riesgo.

Pese a las posibles críticas a la racionalidad de esta prohibición absoluta, desde un punto de vista práctico, conviene detenernos a analizar si dicha prohibición presenta, en la realidad, un efecto útil.

II. REMISIONES AL RGPD, LA OBSOLESCENCIA DEL CONCEPTO DE DATOS SENSIBLES Y SU HERENCIA (SIN BENEFICIO DE INVENTARIO)

La primacía del RGPD como *lex specialis* en lo referente al tratamiento de datos personales responde a un orden natural y lógico para mantener la seguridad jurídica en el marco de la UE. A pesar de esta primacía del RGPD en caso de conflicto, el sistema de relaciones normativas manifiesta una dependencia excesiva del Reglamento, optando por germinar (excesivamente) nuevas normas con conceptos del RGPD. Un claro y problemático ejemplo es la forma de delimitación de los datos sensibles en la prohibición de la DSA.

Si bien tiene completo sentido que la DSA se remita a la definición de datos sensibles ofrecida por el RGPD, la propia incorporación de esta noción en la prohibición de la DSA no resultaba, a nuestro entender, necesaria ni conveniente. Por un lado, porque el legislador de la UE disponía de conceptos mucho más amplios a los que podía haber vinculado la aplicación de la norma, como el de vulnerabilidad. Por otro, porque la configuración de los datos sensibles fue objeto de discordia legislativa desde sus inicios y todo escepticismo sobre su formulación no ha hecho sino incrementarse.

Las razones en que se basan estas arduas críticas, que compartimos, son principalmente dos. La primera es la dificultad de esclarecer con nitidez el criterio seguido para calificar ciertos datos como sensibles, como las convicciones filosóficas (cuya definición y alcance son una incógnita) y excluir otros, como la situación financiera. La segunda, que la técnica ha experimentado un grado de avance hasta un punto en que cualquier dato personal puede ser (o convertirse en) un dato sensible. Se pone en entredicho qué tienen de especial las categorías especiales de datos (denominadas datos sensibles) cuando cualquier dato puede acabar por encajar dentro de este marco y someterse con ello a su regulación especial.

La principal consecuencia del arrastre del concepto de datos sensibles a otras normas es clara. Estas últimas aceptan la noción de datos sensibles sin beneficio de inventario, a pesar de tratarse de una noción que suscita más dudas interpretativas que beneficios aplicativos reales.

Desde una perspectiva práctica, es posible que estas dudas interpretativas afecten no solo a la autoridad competente para abrir investigaciones (la Comisión Europea), sino también a los prestadores de servicios de plataforma. Pasando a un ejemplo concreto: hasta la fecha, el único precedente reseñable ha sido la voluntaria retirada por parte de LinkedIn de una de sus técnicas de personalización publicitaria, a raíz de investigaciones abiertas por la Comisión por un

posible incumplimiento de la referida prohibición de la DSA[1]. Visto así, es posible que la interpretación de la norma (especialmente en lo referente a los datos sensibles) sea profundamente incierta, lo que no resta, en contrapartida, su posible efecto disuasorio, favoreciendo la adopción de medidas voluntarias. Ante la inseguridad jurídica que deriva del concepto podría producirse una aproximación de cumplimiento voluntario por parte de las empresas, que adaptarían el modo en que utilizan los datos a una opción que consideren segura y, con todo, resulte útil para el desarrollo de su actividad.

III. LA NOCIÓN DE PLATAFORMA Y LA INCIERTA REFORMULACIÓN DEL CONCEPTO DE DIFUSIÓN AL PÚBLICO

La estrategia digital de la Unión Europea pone su foco en las denominadas plataformas digitales. Sin embargo, los perfiles que utiliza la normativa para definir estas no son uniformes, como se desprende del distinto sentido que tiene el concepto en la DSA y la DMA. De manera particular, se ha de criticar que el ámbito personal de la prohibición de la DSA excluya a servicios que no sean plataformas en línea pero que, sin embargo, se caractericen por explotar vulnerabilidades de los usuarios. Un ejemplo especialmente problemático de ello es el de los videojuegos en línea, caracterizados por basar su modelo de negocio en la creación de adicciones en sus usuarios para su explotación comercial.

Igualmente, el concepto de plataforma de la DSA plantea no pocos interrogantes derivados del requisito de que el servicio difunda información al público, entendiendo el concepto de público en el nuevo sentido de la DSA. La reformulación de este concepto se plantea problemática por dos razones. La primera, por cuestiones de coherencia en el sistema, ya que este término disfrutaba de una definición consolidada a partir de la jurisprudencia del TJUE. Hubiera sido preferible que la DSA no incorporase una definición propia del concepto de difusión al público, optándose en su lugar por la remisión al concepto de público del TJUE como concepto autónomo de derecho de la UE. Otra alternativa hubiese sido incorporar *verbatim* la definición del TJUE, opción que no es nada insólita en la normativa de la Unión.

Sin embargo, el legislador europeo no adoptó ninguna de estas dos opciones. La consecuencia, además de la incoherencia sistémica, es una mayor inseguridad jurídica sobre si ciertos servicios son o

[1] European Commission, «Statement by Commissioner Breton on steps announced by LinkedIn to comply with DSA provisions on targeted advertisement», Press Release, del 7 de junio de 2024.

no servicios de plataforma. Por contra, el legislador decidió incluir en la DSA una definición propia de público como un número potencialmente ilimitado de terceros. La diferencia es grave: aludir a un número potencialmente *ilimitado*, que no potencialmente *indeterminado* (como se entendía previamente), ha derivado en que el punto de conexión material de la norma se someta a una noción mucho menos flexible. Parece excluir así a servicios que fijen un número máximo de destinatarios, por elevado que pueda ser ese número, si bien sostenemos que esta interpretación no asegura el efecto útil de la norma y puede desencadenar situaciones de fraude de ley.

A nuestro entender, la aclaración del concepto de difusión al público pasará, inevitablemente, por una cuestión prejudicial ante el TJUE. No sería baladí plantearla, puesto que de su esclarecimiento depende no solo la aplicabilidad de la prohibición de la DSA objeto de nuestro estudio, sino de todas aquellas normas dirigidas a las plataformas en línea, como son las referentes a la difusión de contenidos ilícitos, núcleo de la DSA.

IV. LA LISTA DE VLOPS Y LA NO INCLUSIÓN DE LOS SERVICIOS DE INTERMEDIACIÓN PUBLICITARIA

Los principales servicios de intermediación publicitaria (*Alphabet Advertising*, *Meta Ads* y *Amazon Ads*) juegan un papel crucial dentro del mercado único digital, especialmente por su presencia en todo el territorio de la Unión y el amplio alcance de su actividad. Recordemos que, conforme a la DSA, aquellos servicios de plataforma que alcancen o superen los 45 millones de destinatarios activos mensuales dentro del territorio de la Unión deben ser designados como VLOPs por la Comisión Europea. El concepto de destinatarios activos no se limita a quienes interactúan directamente con la publicidad, sino que también abarca a quienes están expuestos a dicha información, incluyendo anunciantes, medios publicitarios y usuarios finales.

Este hecho, sumado a la delimitación de servicios de intermediación publicitaria como servicio diferenciado del servicio principal, nos lleva a plantear que los servicios publicitarios de Alphabet, Meta y Amazon superan ampliamente este umbral cuantitativo al integrar sus servicios publicitarios en interfaces propias y de terceros que han sido previamente designadas como VLOPs, tales como Facebook e Instagram, en el caso de Meta; Amazon Store, en el caso de Amazon; o Google Maps y Google Play, en el caso de Alphabet.

Si bien estos prestadores aún no han diferenciado formalmente sus servicios de intermediación publicitaria respecto de otros servicios principales en sus informes públicos, es evidente que el alcance efectivo de sus anuncios supera considerablemente el umbral estable-

cido por la DSA, cumpliendo así el requisito numérico necesario para ser considerados VLOPs. Su designación implicaría el sometimiento a obligaciones adicionales impuestas por la DSA, lo que serviría para fomentar la apertura de investigaciones por parte de la Comisión sobre el umbral cuantitativo de estos servicios de intermediación publicitaria.

V. LA VIOLACIÓN DE NORMAS POR INFRACCIÓN DEL RGPD Y LAS DIFICULTADES PARA SU APLICACIÓN POR EL JUEZ NACIONAL

La práctica en la aplicación de la violación de normas como acto de competencia desleal se ha desarrollado ligada a conductas *offline*, como la infracción de normas sobre horarios de apertura de comercios. Este instrumento jurídico ha ganado un mayor protagonismo en el ámbito del tratamiento de datos con fines de publicidad *online*, visto el incremento del valor competitivo de los datos. Si bien esta aclaración no era completamente necesaria, el TJUE reafirmó con rotundidad en el caso *Lindenapotheke* que el RGPD no se opone a una normativa nacional que acoja la violación de normas por infracción del citado Reglamento. Con ello se pone de relieve la prospectiva relevancia de esta vía nacional.

Ahora bien, sería razonable calificar de cuando menos difícil la postura del juez nacional cuando examine un supuesto de infracción de normas por incumplimiento del RGPD con fines publicitarios, máxime cuando la infracción alegada es de una complejidad tan profunda como el modelo *pay-or-okay.* Cabe recordar que, en sede de violación de normas, no existe prejudicialidad ni vinculación del juez civil por la calificación que de los hechos hayan podido hacer —en su caso— las autoridades competentes, si bien entendemos que la aproximación del juez nacional no puede ser sino cauta. Este es el fondo del caso de la demanda en España de la Asociación de Medios de Información a Meta. El caso se originó con una demanda en diciembre de 2023, la audiencia previa se celebró en noviembre 2024 y la vista oral ha quedado fijada para octubre de 2025[2]. Esta dilatación temporal, aun usual en el sistema de justicia español, ya denota en cierto modo la complejidad del caso, acorde con los coetáneos pronunciamientos respecto a la legalidad de las bases de tratamiento empleadas por Meta.

Aunque, insistamos, no hay prejudicialidad ni efecto vinculante de la calificación de los hechos que haya hecho una autoridad administrativa, no sería extraño que el juez, en lo respectivo a la apreciación

[2] Información disponible en Poder Judicial España, «La Asociación de Medios de Información reclama 551 millones de euros a Meta por competencia desleal», Comunicación Poder Judicial, 29 de noviembre de 2024.

de una infracción normativa, se alinee con pronunciamientos previos de las autoridades competentes, como es la decisión de la Comisión Europea en la que se sanciona con 200 millones de euros a Meta por la ilicitud del modelo *pay-or-okay* por infracción del art. 5.2 DMA, en relación con las normas sobre consentimiento incluidas en el RGPD. La coherencia del juez nacional con pronunciamientos previos de la Comisión Europea sería prudente, en vista no solo de una coherencia con el sistema de la Unión, sino considerando, por otro lado, que ordenamientos como el alemán también incorporan la violación de normas y sus tribunales pueden enfrentarse a demandas similares. Así las cosas, la resolución judicial de la demanda referida, aun enmarcada a nivel español, podría servir como referente internacional.

VI. LÍMITES A LAS FLEXIBILIZACIONES INTERPRETATIVAS DE LA DPCD

La violación de normas no es el único instrumento jurídico que la competencia desleal ofrece como medida para afrontar la materia aquí tratada. La vía de las prácticas comerciales desleales, en particular las prácticas agresivas, se planteaba por este trabajo y por recientes estudios de la Comisión Europea como una opción para afrontar prácticas no acompasadas por la prohibición de la DSA. La DPCD y su transposición a nuestro ordenamiento cuentan ya con un amplio recorrido que empezaba a plantear dudas sobre su adaptabilidad al alto grado de personalización actual de ciertas prácticas comerciales.

Entre estas disyuntivas estaba el concepto de consumidor medio. Si bien la STJUE *Compass Banca SpA* tiene en cuenta las limitaciones cognitivas de los consumidores, a menudo explotadas mediante sistemas de IA, se cae en el riesgo de someter a los consumidores a una sobreprotección, que tendría como precio la limitación excesiva de las prácticas comerciales y de la libertad de empresa. Otro dilema era la adaptabilidad del concepto de vulnerabilidad de la cláusula general de deslealtad. La literalidad de la cláusula se refiere a aquellas prácticas que puedan distorsionar el comportamiento económico únicamente de «un grupo claramente identificable de consumidores especialmente vulnerables» a dichas prácticas o al producto al que se refieran. Se plantea la duda, ya expuesta por la doctrina, de si dicho precepto es apto para integrar prácticas comerciales basadas en perfiles individuales (altamente personalizadas), donde no concurre un grupo de referencia claramente identificable.

La Comisión Europea, en su guía sobre patrones oscuros, así como parte de la doctrina, aboga por acoger en este precepto no solo a grupos claramente identificables, sino también a consumidores individualmente considerados o, dicho de otra forma, por considerar al consumidor

concreto como un grupo en sí mismo. Si bien la norma puede someterse a criterios interpretativos que la moderen hasta cierto punto, esta flexibilización nos resulta excesiva. La literalidad de la norma guarda un sentido, que no es otro que la seguridad jurídica, y la normativa aplicable presenta, como hemos expuesto, vías alternativas para paliar estas prácticas que no pasen por equiparar un individuo a un grupo.

Pese a la anterior interpretación (que sostenemos contundentemente) podría resultar conveniente, a efectos de claridad normativa, plantear una cuestión prejudicial ante el TJUE, en la que se instase al Tribunal a aclarar la siguiente cuestión:

> ¿Ampara el concepto de «grupo concreto de consumidores» del art. 5.2.b) de la DPCD solo a grupos claramente identificables, o debe entenderse que este concepto acoge también a «consumidores individualmente considerados» cuando la práctica sea muy personalizada o no se pueda señalar claramente a un grupo de referencia?

VII. LA AIA Y LA DPCD: UN MATRIMONIO BIEN AVENIDO

En el referido caso *Compass Banca SpA,* el TJUE subrayó la complementariedad entre la DPCD y la AIA, si bien era razonable (sin necesidad de una cuestión prejudicial) indicar que la AIA resulta de especial aplicación sobre prácticas de IA que fomenten sesgos cognitivos en los destinatarios de prácticas comerciales. Dicho esto, no está de más subrayar dicho carácter complementario, en vista de las virtudes que puede presentar la aplicación de la AIA.

Por un lado, cabe destacar la propia naturaleza de la AIA. Al ser un Reglamento de la UE, es una norma de aplicación directa, por lo que evita los problemas de transposición nacionales que enfrentó la DPCD. Por otro lado, las prohibiciones de técnicas manipulativas, subliminales o explotadoras de vulnerabilidades de la AIA pueden aplicarse teniendo en cuenta al miembro medio del grupo afectado o a una persona física individualmente considerada, lo que sirve para acoger prácticas comerciales de IA tanto segmentadas como extremadamente personalizadas, superando los problemas interpretativos que plantea la DPCD. De igual forma, los ámbitos materiales de dichas prohibiciones evitan la noción del consumidor medio, lo que sirve para concluir que el legislador de la UE puede formular nuevas propuestas legislativas que no dependan de conceptos problemáticos incorporados en normas precedentes.

VIII. QUÉ ES SER VULNERABLES, SI TODOS SOMOS VULNERABLES

El concepto de vulnerabilidad se ha mencionado en no pocas ocasiones a lo largo del presente examen. Entre ellas, al justificar la razón de ser de la regulación de datos sensibles y de la prohibición de la DSA; al considerar las prácticas comerciales desleales bajo el prisma de la cláusula general de deslealtad; y al analizar la homónima prohibición de sistemas de IA que exploten vulnerabilidades, si bien este concepto encuentra también su conexión con las prácticas de IA manipuladoras y subliminales.

La vulnerabilidad se ha transformado en un factor clave en la regulación del mercado único digital y de las relaciones que en ella rigen. A nuestro entender, de este concepto se derivan tres reflexiones interconectadas. La primera, que no hay un claro consenso sobre qué es la vulnerabilidad, ni en el propio marco normativo, ni en el jurisprudencial, ni en el doctrinal. La segunda, que la vulnerabilidad ha pasado a ser un concepto jurídico indeterminado, formando parte de un elenco compuesto por nociones como la buena fe, el interés general, la esencialidad, la moral, o la urgencia. La tercera, derivada de la anterior, es que esta configuración como un concepto jurídico indeterminado no obsta (es más, exige) descender de la abstracción a la particularización. Parafraseando a García de Enterría, nos referimos a «supuestos de hecho o áreas de intereses o de actuación perfectamente identificables […] existe un límite a la indeterminación, y un límite manifiesto y patente, nada impreciso, ambiguo o vaporoso, un límite rotundo»[3]. La vulnerabilidad, como todo concepto jurídico indeterminado, demanda una acción que configura el propio sentido del derecho: aplicar las generalizaciones al caso concreto y real.

En suma, la apreciación de la vulnerabilidad no es sino otra forma de considerar las circunstancias y de aplicar un examen casuístico, actividad que carece de novedad en la tradición jurídica y que configura la propia naturaleza de la aplicación del derecho, lo que determina que toda persona, en determinados casos, puede llegar a ser vulnerable.

IX. LA HIPERREGULACIÓN DE LAS PRÁCTICAS COMERCIALES PERSONALIZADAS

La conclusión evidente del presente trabajo es la hiperregulación existente sobre las prácticas comerciales personalizadas. Este fenó-

[3] García de Enterría, «Una nota sobre el interés general como concepto jurídico indeterminado», *Revista española de derecho administrativo*, núm. 89, 1996, p. 83.

meno tiene como ejemplos la DSA, la DMA, el RGPD, la normativa de transposición de la DPCD y la AIA, por no mencionar que, si nos encontrásemos ante anuncios sobre productos o servicios especiales (como el alcohol, los cosméticos o los juegos de azar), el examen se complicaría aún más.

Esta hiperregulación se traduce en las dificultades, a efectos de compliance, que atraviesan los diversos operadores participantes en la personalización de prácticas comerciales. Si bien estas medidas tienen como objeto crear un entorno digital más seguro y respetuoso con los derechos de los destinatarios, los prestadores de servicios son sometidos a crecientes obligaciones de prevención y gestión de riesgos, incluyendo el establecimiento de altos requisitos técnicos (y costosos) que aseguren el uso de sistemas automatizados transparentes y explicables. A ello se suma la posible aplicación de multiplicidad de sanciones derivadas de estas normas, donde la aplicación de los principios de proporcionalidad y ne bis in idem no siempre resulta clara, teniendo como consecuencia general la inseguridad jurídica, así como, previsiblemente, excesivas intromisiones sobre el mercado único digital.

Todo ello nos lleva a concluir con una reflexión (abierta) sobre si esta hiperregulación es proporcionada, beneficiosa y útil para el sistema de la UE, sin olvidar que la misma no solo afectará a este sistema, en vista del (de largo conocido) efecto Bruselas.

BIBLIOGRAFÍA

1. Doctrina

Aido Vázquez, A. M. «La delimitación de los mercados digitales: una aproximación a la nueva comunicación de la Comisión Europea», en Tato Plaza, A.; Costas Comesaña, J.; Fernández Carballo-Calero, P.; Louredo Casado, S.; Torres Pérez, F. J. (coords.*), Nuevas tendencias en el Derecho de la Competencia y de la Propiedad Industrial e Intelectual IV*, 2024, pp. 27-66.

Albarrak, L., Metatla, O. y Roudaut, A. «Exploring the influence of subliminal stimulus type and peripheral angle on the priming effect», *International Journal of Human – Computer Studies 151*, 2021.

Alfaro Águila-Real, J. «Competencia desleal por infracción de normas», *Revista de Derecho Mercantil*, 202, 1991.

Amedeo, A. «The Twin Doctrines of Primacy and Pre-Emption», en Schütze, R. y Tridimas, T., *Oxford Principles of European Union Law: The European Union Legal Order: Volume I,* Oxford Academic, 2018, pp. 300-349.

Ariely, D. *Predictably irrational: the hidden forces that shape our decisions*, HarperCollins, 2010.

Bania, K. «Fitting the Digital Markets Act in the Existing Legal framework: the Myth of the Without Prejudice Clause», *European Competition Journal*, 19(1), 2023.

Barona Vilar, S. «Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale», *Actualidad Jurídica Iberoamericana*, núm. 21, 2024.

Barrio Andrés, M. «Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial», en Barrio Andrés, M. (dir.), *El Reglamento de Inteligencia Artificial*, Tirant lo Blanch, 2024, pp. 30-40.

Basozabal Arrue, X. «La subsidiariedad de la acción de enriquecimiento injusto», *Almacén de Derecho,* 2019, versión *online*.

Becker, S. y Penfrat, J. «The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful», en Van Hoboken, J. *et al.*, *Putting the Digital Services Act into Practice. Enforcement, Access to Justice, and Global Implications*, Verfassungsbooks, 2023, pp. 53-62.

Benavides Velasco, P. «Los sujetos (III): consumidores y usuarios ante el reto de la economía colaborativa», en Gosálbez Pequeño, H. *(dir.), Régimen jurídico del consumo colaborativ*o, 2019, ISBN 978-84-1309-239-3, pp. 163-183.

— «The position of the Court of Justice of the European Union on services provided by digital platforms in the tourism sector», en *Journal of Tourism and Heritage Research: JTHR,* ISSN-e 2659-3580, vol. 4, núm. 2, 2021 (Ejemplar dedicado a: Journal of Tourism and Heritage Research), pp. 189-209.

Beneyto Pallás, K. «Acciones, legitimación y prescripción en materia de competencia desleal», en Beneyto Pallás, K. (dir.), *Actos de competencia desleal y su tratamiento procesal: un estudio práctico de la Ley de competencia desleal (LCD)*, Tirant lo Blanch, 2020, pp. 271-289.

Bennis, S. «AI and the Consumer», en Savin, A. y Trzaskowski, J., *Research Handbook on EU Internet Law*, 2nd ed., Edward Elgar, 2023, pp. 101-136.

— «AI and the Consumer», en Savin, A.; Trzaskowski, J. (eds.), *Research Handbook on EU Internet Law*, Edward Elgar, 2023, pp. 468-485.

Bercovitz-Rodríguez Cano, A. *Apuntes de derecho mercantil*, Aranzadi, 2021.

— «Nociones introductorias», en Bercovitz Rodríguez-Cano, A. (dir.), *Comentarios a la ley de competencia desleal*, Aranzadi, 2011.

Bermúdez, J. P. *et al.*, «What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence», *IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, 2023.

BEUC. «Dark Patterns and the EU Consumer Law Acquis», *BEUC Position Paper*, 2022.

Boine, C. «The AI Manipulation Gap», *SSRN Electronic Journal*, 2021.

Bongard-Blanchy, K. *et al.*, «I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!» – Dark Patterns from the End-User Perspective, *Proceedings of the 2021 ACM Designing Interactive Systems Conference 763*, 2021.

Botta, M. «Compliance with the DMA obligations: the prohibition of data combination under art. 5(2) DMA», en Ruiz Peris, J. I y Estevan de Quesada, C., *New European Competition Trends in Digital Markets*, Atelier, 2024, pp. 259-280.

Botta, M. y Wiedemann, K. «To Discriminate or Not to Discriminate? Personalised Pricing in Online Markets as Exploitative Abuse of Dominance», *European Journal of Law and Economics*, 50, 2020.

Bourreau, M., *et al.,* «Big Data and Competition Policy: Market power, personalised pricing and advertising», *SSRN Electronic Journal*, 2019.

Boyan, B. «Modern Trends in Automatic Generation of Content for Video Games», *Serdica Journal of Computing*, 2019.

Braganza, A. «The Challenges of Artificial Intelligence», *International Corporate Rescue*, 15(2), 2018.

Burak Alakus, T., Gonen, M. y Turkoglu, I. «Database for an emotion recognition system based on EEG signals and various computer games – GAMEEMO», *Biomedical Signal Processing and Control*, vol. 60, 2020.

Bush, C. y Fletcher, A. «Harmful Online Choice Architecture: How Digital Design Can Harm Consumers and Undermine the Consumer Acquis», *CERRE*, 2022.

Calabresi, G. «Ideals, Beliefs, Attitudes, and the Law: Private Law Perspectives on a Public Law Problem», *Syracuse University Press,* 1995.

Calo, R. «Digital market manipulation», *82 George Washington Law Review 995*, 2014.

Calvo, R. A., Peters, D., Vold, K., y Ryan, R. M. «Supporting human autonomy in AI systems: A framework for ethical enquiry», en *Ethics of Digital Well-Being*, Springer, 2020, pp. 31-54.

Calvo, R., Peters, D., Johnson, D. y Rogers, Y. «Autonomy in technology design», in *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, 2014.

Candrian, C., Scherer, A., «Rise of the machines: Delegating decisions to autonomous AI» *Computers in Human Behavior,* vol. 134, 2022, disponible en *https://doi.org/10.1016/j.chb.2022.107308*.

Carbajo Cascón, F. «Violación de secretos, inducción y aprovechamiento de la infracción contractual e infracción de normas», en García-Cruces González, J. A. (coord.), *Tratado de Derecho de la competencia y de la publicidad*, vol. 2, Tirant lo Blanch, 2014, pp. 1525-1622.

Castillo Parrilla, J. A. «Pay or ok. Pagar con datos personales tras la Directiva 2019/770: una visión comparada entre España y Portugal», *Revista Electrónica de Direito*, 2024.

— «Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial», *Derecho Privado y Constitución*, 43, 2023.

Celis, E., Mehrotra, A. y Vishnoi, N. «Toward Controlling Discrimination in Online Ad Auctions», *International Conference on Machine Learning*, 2019.

Cennamo, C. *et al.,* «Digital Platforms Regulation: An Innovation Centric View of the EU's Digital Markets Act», *Journal of European Competition Law & Practice*, 2023.

Chang, Y., Winston, C. y Yan, J. «Does Uber Benefit Travelers by Price Discrimination?», *The Journal of Law and Economics,* 2018.

Cialdini, R. B. «Harnessing the Science of Persuasion», *Harvard Business Law Review*, 2001.

Cohen, T. «Regulating Manipulative Artificial Intelligence», *SCRIPTed – A Journal of Law, Technology & Society*, 2023.

Colangelo, G. y Maggiolino, M. «Data Protection in Attention Markets: Protecting Privacy through Competition?», *Journal of European Competition Law & Practice*, vol. 8, núm. 6, 2017.

— «From fragile to smart consumers: Shifting paradigm for the digital era», Computer Law & Security Review, vol. 35, núm. 2, 2019.

Collins, H. «Harmonisation by example: European Laws against Unfair Commercial Practices», *The Modern Law Review*, 2010.

Comisión Europea, *Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*, 2020.

Costas Comesaña, J. «Prohibición de falseamiento de la libre competencia por actos de competencia desleal», en Bello Martín-Crespo, M. P.; Hernández Rodríguez, F. (coords.) y Gómez Segade, J. A. (pr.), *Derecho de la libre competencia comunitario y español*, 2009, pp. 213-232.

Czarnocki, J. «Will new definitions of emotion recognition and biometric data hamper the objectives of the proposed AI Act?», *International Conference of the Biometrics Special Interest Group (BIOSIG),* 2021.

De Pelsmacker, P. «How advertising works», en *Advanced Introduction to Advertising*, pp. 65-75.

De Streel, A. y Hocepied, C. «The Regulation of Electronic Communications Networks and Services», en Garzaniti, L., O'Regan, M., De Streel, A. y Valcke, P., *Electronic Communications, Audiovisual Services and the Internet*, Sweet and Maxwell, 2019, pp. 25-123.

De Streel, A. y Jacques, F. «Personalised pricing and EU law», *30th European Conference of the International Telecommunications Society (ITS)*, 2019.

De Torres Perea, J. M. «La patrimonialización de datos ante la contaminación digital. Una perspectiva civil ante un reto a nuestro sistema», *Revista de Derecho Civil*, vol. xii, núm. 1, 2025.

Di Porto, F. *et al.,* «I see something you don't see. A computational analysis of the DMA and DSA», *Computational Antitrust Journal*, 2021.

Di Porto, F.; Egberts, A. «The Collective Welfare Dimension of Dark Patterns Regulation», European Law Journal, 2023.

Diéguez Aguilera, L. «El consumidor vulnerable: en especial, la vulnerabilidad de las personas mayores ante la acusada digitalización del mercado financiero», *Diario La Ley*, 2023.

Díez Estella, F. «El art. 3 LDC: falseamiento de la competencia por actos desleales», en Beneyto Pérez, J. M. (dir.) y Maillo González-Orús, J. (dir.), *Tratado de derecho de la competencia: Unión Europea y España*, vol. 1, tomo 1, 2017, pp. 505-553.

Dileo, D. «Aristotle's manipulative maxim», *Rev Pol*, 82(3), 2020.

Dinwoodie, G. B.; Gangjee, D. S. «The Image of the Consumer in European Trade Mark Law», en Leczykiewicz, D.; Weatherill, S. (eds.), *The Image(s) of the Consumer in EU Law*, Hart Publishing, 2015, pp. 34-35.

Dobber, T., Ó; Fathaigh, R. y Zuiderveen Borgesius, F. J. «The regulation of online political micro-targeting in Europe», *Internet Policy Review*, 8(4), 2019.

Duivenvoorde, B. y Goanta, C. «The regulation of digital advertising under the DSA: A critical assessment», *Computer Law & Security Review*, 51, 2023.

Duivenvoorde, B. *The Consumer Benchmarks in the Unfair Commercial Practices Directive*, Springer, 2016.

Ebers, M. y Sein, K. «Data-driven Technologies – Challenges for Privacy and EU Data Protection Law», en Ebers, M. y Sein, K., *Privacy, Data Protection and Data-driven Technologies*, Routledge, 2024, pp. 16-23.

Emparanza Sobejano, A. «Artículo 15. Violación de normas», en Martínez Sanz, F., *Comentario práctico a la Ley de Competencia Desleal,* Tecnos, 2009, pp. 255-272.

Esplugues García, J. «La infracompensación como excepción al deber de limitar el daño», en *Revista Aranzadi de Derecho Patrimonial*, núm. 63, 2024.

Esposito, F. y Maciel Cathoud Ferreira, T. «Addictive design as an unfair commercial practice: the case of hyper-engaging dark patterns», *European Journal of Risk Regulation*, 2024, pp.1000-1016.

Estevan de Quesada, C. «Data-protection related abuses by digital platforms: a Spanish enforcement alternative», en Ruiz Peris, J. I. y Estevan de Quesada, C., *New European Competition Trends in Digital Markets*, Atelier, 2024, pp. 281-303.

European Commission. *Understanding Consumer Vulnerability in the EU's Key Markets*, 2016.

Farrel, J. «Can privacy be just another good?», *Journal on Telecommunications and High Technology Law*, 2012.

Fernández Carballo-Calero, P. «Aggressive Commercial Practices in the Case Law of EU Member States*», Journal of European Consumer and Market Law*, vol. 5, núm. 6, 2016.

Fernández Carballo-Calero, P. I. «Concetto e caratteri generali», en Fernández Carballo-Calero, P. I. *Pubblicità occulta e product placement*, Cedam, 2024, pp. 3-6.

Fernández Nóvoa, C. «La publicidad encubierta», en E*studios de Derecho de la Publicidad*, Universidad de Santiago de Compostela, 1989, pp. 189 y ss.

Franck, J. y Purnhagen, K., «Homo economicus, behavioural sciences, and economic regulation: On the concept of man in internal market regulation and its normative basis», en Mathis, K. (ed.), *Law and Economics in Europe*, Springer, 2014.

Frosio, G. y Geiger, C. «Taking fundamental rights seriously in the Digital Services Act's platforms liability regime», *European Law Journal*, vol. 29, 2023.

Furman, J., Coyle, D., Fletcher, A., Marsden, P. y Mcauley, D., *Unlocking digital competition. Report of the Digital Competition Expert Panel (Furman Report),* 2019.

Galacho Abolafio, A. F. «Contenidos digitales y su puesta a disposición a través de Internet a la luz de las últimas sentencias del TJUE: el papel fundamental del concepto de agotamiento del Derecho», en Miranda Serrano, L. M. y Pagador López, J. (dirs.); Serrano Cañas, J. M.; Casado Navarro, A. y González Jiménez, P. M. (coords.), *Contratación mercantil: digitalización y protección del cliente-consumidor*, 2023, pp. 75-92.

— «El reconocimiento de la distribución digital para determinados actos de comunicación pública», *Actas de Derecho Industrial y Derecho de Autor*, tomo 43, 2023.

Galli, F. «Predictive Personalisation», en Galli, F., *Algorithmic Marketing and EU Law on Unfair Commercial Practices*, Law, Governance and Technology Series, volume 50, 2022, pp. 81-107.

García Álvarez, P. «Aplicación de redes neuronales en la predicción de mortalidad por neumonía», *SciELO*, 2020.

García de Enterría Martínez-Carande, E. «Una nota sobre el interés general como concepto jurídico indeterminado», *Revista Española de Derecho Administrativo*, núm. 89, 1996.

Geradin, D. y Katsifis, D., «An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age», *TILEC Discussion Paper No. DP2019-031*, 12 de diciembre 2018.

Geradin, D. y Petit, N., «Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles», *Global Competition Law Centre Working Paper Series núm. 07/05*, 2015.

Gómez Sánchez, Y. «Categorías especiales de datos personales: los datos de origen étnico o racial, los datos genéticos, los datos biométricos, los datos relativos a la salud, los datos relativos a la vida sexual y a la orientación sexual (comentario al art. 9.1. RGPD)», en Troncoso Reigada, A., *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales,* tomo i, Aranzadi, 2021, pp. 1041-1058.

González Cabañas, J., Cuevas, A. y Cuevas, R. «Facebook use of sensitive data for advertising in Europe», *27th USENIX Security Symposium*, 2018.

Gualda Alcalá, F. J. «Los datos que revelen la afiliación sindical como categoría especial de datos personales (comentario al artículo 9.1. RGPD)», en Troncoso Reigada, A., *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales,* Tomo i, Aranzadi, 2021, pp. 1095-1108.

Gumbus, A. y Grodzinsky, F. «Era of Big Data: Danger of Discrimination», *SIGCAS Computers & Society,* vol. 45, núm. 3, 2016.

Hacker, P. «Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law», *European Law Journal*, 2021.

Hanson, J. D. y Kysar, D. «Taking Behavioralism Seriously: Some Evidence of Market Manipulation», *Harvard Law Review*, vol. 112, núm. 7, 1999.

Heawood, J. «Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal», *Information Polity*, 2018.

Helberger, N. «Profiling and targeting consumers in the Internet of Things; a new challenge for consumer law», en Schulze, R. y Staudenmayer, D. (eds.), *Digital revolution: challenges for contract law in practice*, Nomos Baden-Baden, 2016, versión *online*.

Helberger, N. *et al.,* EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets, BEUC – The European Consumer Organisation, 2021.

Hermanus, D. R. *et al.,* «Unveiling the Power of ChatGPT: Transforming Face Detection with AI and AR», *10th International Conference on ICT for Smart Society (ICISS)*, 2023.

Herring, J. «Foreword: Vulnerability and the Law», *University of New South Wales Law Journal*, 41(3), 2018.

Herrera Petrus, C. *et al.,* «Acciones frente a la competencia desleal», en Tato Plaza, A., Fernández Carballo-Calero, P. y Herrera Petrus, C., L*a reforma de la ley de competencia desleal*, La Ley Wolters Kluwer, 2010, pp. 283-290.

Hinds, J., Williams, E. J. y Joinson, A. N. «"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal», *International Journal of Human-Computer Studies*, vol. 143, 2020.

Hobbelen, H., Cunningham, F. y Denihan, C. «The European Commission's Ambitious Regulatory Agenda in the Field of Digital Services and AI: a status update from Brussels on the DSA, DMA and AI Act», *IBA*, 2021.
Huergo Lora, A. «Una aproximación a los algoritmos desde el Derecho Administrativo», en Huergo Lora, A. y Díaz González, G., *La regulación de los algoritmos*, Aranzadi, 2020, pp. 23-59.
Husovec, M. «Principles», en *Principles of the Digital Services Act,* Oxford Academic, 2024, pp. 465-478.
— «The DSA's Scope Briefly Explained», *SSRN Electronic Journal*, 2023.
Husovec, M. y Roche Laguna, I. «Digital Services Act: A Short Primer», *SSRN Electronic Journal*, 2022.
Ienca, M. «On Artificial Intelligence and Manipulation», *Topoi*, 42, 2023.
Incardona, R. y Poncibò, C. «The average consumer, the unfair commercial practices directive, and the cognitive revolution», *Journal of Consumer Policy*, vol. 30, 2007.
Jacobs, N. «Two Ethical Concerns about the Use of Persuasive Technology for Vulnerable People», *Bioethics*, 34(5), 2020.
Jasserand, C.A. «Avoiding Terminological Confusion between the Notions of 'biometrics' and 'biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective», *International Data Privacy Law,* vol. 6, 1, 2015.
Jobin, A., Ienca, M. y Vayena, E. «The global landscape of AI ethics guidelines», *Nature Machine Intelligence*, 2019, vol. 1, núm. 9.
Jolls, C. *et al.,* «A Behavioral Approach to Law and Economics», *Stanford Law Review*, vol. 50, 1998.
Joost, P. y Zuiderveen, B., «Personalised Pricing: The Demise of the Fixed Price?», en Kohl, U. y Eisler, J. (eds.), *Data-Driven Personalisation in Markets, Politics and Law,* Cambridge University Press, 2021.
Kaprou, E. «Aggressive Commercial Practices 2.0: Is the UCPD Fit for the Digital Age?», Journal of European Consumer and Market Law, vol. 12, núm. 2, 2023.
Kartali, A., Roglić, M., Barjaktarović, M., Đurić-Jovičić, M. y Janković, M. «Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches», *14th Symposium on Neural Networks and Applications (NEUREL)*, 2018.
Kindt, E. J. «Having yes, using no? About the new legal regime for biometric data», *Computer Law and Security Review*, 34, 2017.
— «Por qué la investigación puede ya no ser la misma: sobre el alcance territorial de la propuesta de Reglamento de Protección de Datos», *Documento de Trabajo 26/2016 del CiTiP*, pp. 13-29.
— «Why research may no longer be the same: about the territorial scope of the Proposed Data Protection Regulation», *CiTiP Working Paper 26/2016*, 2016.
— *Privacy and data protection issues of biometric applications. A comparative legal analysis*, Springer, 2013.
Kollmer, T. y Eckhardt, A. «Dark Patterns: Conceptualization and Future Research Directions», *Business & Information Systems Engineering*, 65, 2022.

Kosinski, M., Stillwell, D. y Graepel, T. «Private traits and attributes are predictable from digital records of human behavior», *Proceedings of the National Academy of Sciences (PNAS)*, 2013.

Krämer, J., Schnurr, D. y Broughton Micova, S. «The Role of Data for Digital Markets Contestability», *CERRE Report*, 2020.

Krook, J. «Manipulation and the AI Act: Large Language Model Chatbots and the Danger of Mirrors», *SSRN Electronic Journal*, 2024, disponible en *https://ssrn.com/abstract=4719835.*

Kumar, A., Shetty, P., Balipa, M., Rao, B., Puneeth, B. y Shravya, «An efficient technique to detect skin disease Using Image Processing», *2022 International Conference on Artificial Intelligence and Data Engineering (AIDE)*, 2022.

Kupčík, J. y Mikeš, S. «Discussion on big data, online advertising and competition policy», *European Competition Law Review*, 2018.

Laustsen, R. D. «The Average Consumer in Confusion-Based Disputes in European Trademark Law and Similar Fictions», en *The Average Consumer: A Consumer Fiction in European Trademark Law*, Springer, 2020.

Lema Devesa, C. y Fernández Carballo-Calero, P. «La represión de la competencia desleal», en Jiménez Sánchez, G. J. y Díaz Moreno, A. (coords.), Derecho Mercantil: vol. 2. Derecho industrial. Propiedad industrial. Explotación empresarial de la propiedad intelectual. Régimen jurídico de la competencia, 2013, pp. 235-256.

— «Las prácticas publicitarias engañosas en la Directiva de 11 de mayo de 2005», en Comunicaciones en propiedad industrial y derecho de la competencia, núm. 46 (abril-junio), 2007, pp. 77-90.

Lessig, L. «The code of Privacy», *Proceedings of the American Philosophical Society*, vol. 151, 2007.

— *Code 2.0*, CreateSpace Independent Publishing Platform, 2009.

Limongelli, R. «Caveat Emptor de AI, from Black Box to Glass Box: Reviewing Consumer Protection against AI-Enabled Manipulation in the European Union», *SSRN Electronic Journal*, 2023.

Louredo Casado, L. «El posible carácter desleal e injusto de los precios personalizados en internet», D*erecho Digital e Innovación. Digital Law and Innovation Review*, 7, 2020.

Ludmila, G. y Kuner, C. «Article 9 Processing of special categories of personal data», en Kuner, C. *et al.*, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, 2020, pp. 365-385.

Luguri, J. y Strahilevitz, L. J. «Shining a Light on Dark Patterns», Journal of Legal Analysis, vol. 13, núm. 1, 2021.

Lynskey, O. «Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens», *European Law Review*, 2011.

Maas, M. M. «Concepts in Advanced AI Governance: A Literature Review of Key Terms and Definitions», *SSRN Electronic Journal*, 2023.

Malgieri, G. «Data protection principles and vulnerable data subjects», en Malgieri, G., *Vulnerability and Data Protection Law*, Oxford University Press, 2023, pp. 101-129.

Malgieri, G. y Comandé, G. «Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era», *Information, Communication and Technology Law*, Issue 3, 2017.

Malgieri, G. y Pasquale, F. A. «From Transparency to Justification: Toward Ex Ante Accountability for AI», *Brooklyn Law School, Legal Studies Paper No. 712, Brussels Privacy Hub Working Paper,* núm. 33, 2022.

Malgieri, G. y Quinn, P. «The Difficulty of Defining Sensitive Data. The concept of sensitive data in the EU data Protection framework», *German Law Journal*, 2020.

Márquez Lobillo, P. «El contrato de intermediación electrónica tras los reglamentos europeos sobre transparencia y equidad (P2B), servicios y mercados digitales», *Revista de derecho mercantil*, núm. 334, 2024.

Martí Miravalls, J. «La responsabilidad civil por infracción del Derecho de la Competencia», en CEFLegal: Revista práctica de derecho. Comentarios y casos prácticos, núm. 225, 2019.

— «Acciones de daños por infracción del derecho de la competencia: responsabilidad conjunta y prescripción», en Actas de derecho industrial y derecho de autor, tomo 37, 2016-2017.

Martínez-Torrón, J. «La protección internacional de la libertad religiosa y de conciencia, cincuenta años después», *Revista de la Facultad de Derecho de la Universidad de Granada*, 1999.

Massaguer Fuentes, J. «Ámbito de aplicación de la Directiva», en Massaguer Fuentes, J., *El nuevo derecho contra la competencia desleal: La Directiva 2005/29/CE sobre las prácticas comerciales desleales*, Civitas, 2006, pp. 1-30.

— «Artículo 15. Violación de Normas», en Massaguer Fuentes, J., *Comentario a la Ley de Competencia Desleal*, Civitas, 1999, pp. 292-318.

— «La prohibición general de las prácticas comerciales desleales», en Massaguer Fuentes, J., *El nuevo derecho contra la competencia desleal: La Directiva 2005/29/CE sobre las prácticas comerciales desleales*, Civitas, 2006, pp. 57-98.

— «Las prácticas comerciales agresivas», en Massaguer Fuentes, J., *El nuevo derecho contra la competencia desleal: La Directiva 2005/29/CE sobre las prácticas comerciales desleales*, Civitas, 2006, pp. 131-138.

— «Principios generales», en Massaguer Fuentes, J., *El nuevo derecho contra la competencia desleal: La Directiva 2005/29/CE sobre las prácticas comerciales desleales*, Civitas, 2006, pp. 33-52.

— *El nuevo Derecho contra la Competencia Desleal. La Directiva 2005/29/CE sobre las Prácticas Comerciales Desleales*, Civitas, 2006.

Mccullagh, K. «Data Sensitivity: Proposals for Resolving the Conundrum», *Journal of International Commercial Law and Technology*, vol. 2, Issue 4, 2007.

Menéndez Menéndez, A. *La competencia desleal*, Madrid, Civitas, 1988.

Mercader Uguina, J. R. «Discriminación algorítmica y derecho granular: nuevos retos para la igualdad en la era del big data», Labos: Revista de Derecho del Trabajo y Protección Social, vol. 2, núm. 2, 2021.

Minervini, E.; Rossi Carleo, L. *Le pratiche commerciali sleali: direttiva comunitaria ed ordinamento italiano,* A. Giuffrè, 2007.

Miranda Anguita, A. «La letra pequeña de la publicidad ante el derecho de la competencia desleal», en Serrano Cañas, J. M.; Casado Navarro, A.; González Jiménez, P. M. (coords.); Miranda Serrano, L. M. y Pagador López, J. (dirs.), *Desafíos del regulador mercantil en materia de contratación y competencia empresarial*, 2021, pp. 507-522.

Miranda Serrano, L. M. «Algunas cuestiones controvertidas de las relaciones entre la normativa contractual de consumo y la reguladora de las prácticas desleales contra los consumidores», *La Ley mercantil*, núm. 110, 2024.

— «Economía colaborativa y competencia desleal: ¿deslealtad por violación de normas a través de la prestación de servicios facilitados por plataformas digitales?», *Revista de Estudios Europeos,* núm. 70, 2017.

Miranda Serrano, L. M. y Pagador López, J. «Misleading and Aggressive Commercial Practices and Defects of Transactional Consent», en Schulze, R. y Perales Viscasillas, M. del P. (coords*.), The Formation of Contract: New Features and Developments in Contracting*, 2016, pp. 89-108.

Moreno Belloso, N. y Petit, N. «The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove», *European Law Review*, 391, 2023.

Murry, C. *et al.,* «Price Discrimination in International Airline Markets», *The Review of Economic Studies,* 2019, versión *online*.

Muruaga Herrero, P. «Tres cuestiones en torno a la indemnización de daños y perjuicios en la apropiación de secretos empresariales: información secreta, requisitos de la acción y lucro cesante», en *Pe. i.: Revista de Propiedad Intelectual*, núm. 75, 2023, pp. 63-65.

Narciso, M. «The Unfair Commercial Practices Directive – Fit for Digital Challenges?», *Journal of European Consumer and Market Law*, 4, 2024, pp. 147-153.

Navarro Parra, C. «Daños y perjuicios ante la conducta desleal: criterios para su cálculo», en Bercovitz Rodríguez-Cano, A. (dir.*), Comentarios a la ley de competencia desleal, Aranzadi,* 2011, pp. 315-318.

Nišević, M., *Profiling through Big Data Analytics*, Intersentia, 2023.

Noto La Diega, G. «Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information», *JIPITEC*, 2018.

Novelli, C.; Casolari, F.; Hacker, P.; Spedicato, G.; Floridi, L. «Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity», *Computer Law & Security Review,* vol. 55, 2024, art. núm. 106066.

Núñez Seoane, J. «El derecho de la información y acceso al funcionamiento de los algoritmos que tratan datos personales», en Huergo Lora, A., *La regulación de los algoritmos*, Thomson Reuters Aranzadi, 2020, pp. 299-315.

Oddleifson, E. «The effects of modern data analytics in electoral politics: Cambridge Analytica's Suppression of Voter Agency and the implications for global politics», *Political Science Undergraduate Review*, 2020.

OECD. Dark Commercial Patterns, OECD Digital Economy Papers, núm. 336, 2022.

Olmedo Peralta, E. «Colaboración en la generación, intercambio y procesamiento de datos (big data): entre la cooperación lícita y las conductas antitrust», en Gómez Asensio, C. (coord.); Ruiz Peris, J. I. y Estevan de Quesada, C. (dirs.), *Cooperación y mercados digitales*, Atelier, 2023, pp. 107-144.

— «Condiciones para la concesión de licencias sobre el sistema operativo móvil Android: Tying, self-preferencing y acuerdos de reparto de ingresos

por publicidad (revenue sharing agreements)», *Actas de derecho industrial y derecho de autor*, tomo 44, 2024.

— «El reto de adaptar el derecho de la competencia a la lógica de la economía de los datos», en Olmedo Peralta, E. (dir.), *La aplicación del derecho de la competencia en la economía de los datos*, Aranzadi, 2021.

— «Entornos Informáticos: Sistemas Operativos, Tiendas de Aplicaciones, Asistentes Virtuales y Aplicaciones», en Montero Pascual, J. J. (coord.), *La regulación de los servicios digitales,* Tirant lo Blanch, 2024, pp. 349-406.

— «How does Android protect its dominance in the mobile ecosystem, and why might the Digital Markets Act not be enough? Concerns on Alphabet practices on operating system», en Ruiz Peris, J. I. y Estevan de Quesada, C., *New European Competition Trends in Digital Markets*, Atelier, 2024, pp. 209-235.

— «La construcción de un régimen jurídico para el sector digital más allá del reglamento de mercados digitales», en Rodilla Martí, C. y Ruiz Peris, J. I. (coords.), *Mercados digitales y competencia,* Tirant lo Blanch, 2022, pp. 153-208.

— «Las plataformas de economía colaborativa ante la propuesta de ley de mercados digitales: ¿Son suficientemente disputables los mercados colaborativos?», en Serrano Cañas, J. M.; Casado Navarro, A.; González Jiménez, P. M. (coords.); Miranda Serrano, L. M. y Pagador López, J. (dirs.), *Desafíos del regulador mercantil en materia de contratación y competencia empresaria*l, Marcial Pons, 2021, pp. 359-380.

— «Redefiniendo el ámbito de aplicación de la Ley de Mercados Digitales: ¿a quién?, ¿cómo? y ¿para qué?», en Tato Plaza, A., Costas Comesaña, J., Fernández Carballo-Calero, P., Torres Pérez, F. J. y Louredo Casado, S. (dirs.), *Nuevas tendencias en el derecho de la competencia y de la propiedad industrial III,* 2022, Comares, pp. 87-116.

Otero Cobos, M. T. «El uso de información por los guardianes de acceso sobre transacciones de terceros», en Olmedo Peralta, E. y Robles Martín-Laborda, A. (coords.), *Estudios de la red académica de defensa de la competencia (RADC),* 2022.

Palau Ramírez, F. «Actos concretos de competencia desleal (I): por contrariar las exigencias de la buena fe; por explotación de la reputación ajena; por inducción a la infracción contractual; por violación de normas (arts. 4, 12, 14 y 15 LCD)», en Armengor Vilaplana, A. (coord.) y Beneyto Pallás, K. (dir.), *Actos de competencia desleal y su tratamiento procesal: un estudio práctico de la Ley de competencia desleal (LCD)*, Tirant lo Blanch, 2020, pp. 19-72.

— «La proyectada legislación alemana contra la competencia desleal y su valoración a partir de la legislación española», Estudios sobre consumo, núm. 67, 2003, pp. 27-51.

Paniagua Zurera, M. y Miranda Serrano, L. M. «La protección de los consumidores y usuarios y la irrupción del derecho de los consumidores», en Miranda Serrano, L. M.; Pagador López, J. (coords.), *Derecho (privado) de los consumidores*, 2012, pp. 19-62.

Pastrana Espárraga, M. «Los precios personalizados como práctica anticompetitiva de discriminación mediante el uso de algoritmos», en Paniagua Zurera, M. (dir.), Cruz Ángeles, J.; Martín Ríos, B.; Novo Foncu-

BIERTA, M. (coords.), *El sistema jurídico ante la digitalización: estudios de derecho privado*, 2021, pp. 361-378.

— *Restricciones a la competencia mediante algoritmos en mercados digitales*, Tirant lo Blanch, Valencia, 2025.

PEINADO GRACIA, J. I. «La propiedad intelectual: derechos de autor y derechos afines», en MENÉNDEZ MENÉNDEZ, A. y ROJO FERNÁNDEZ RÍO, A. J. (dirs.), *Lecciones de derecho mercantil*, 2024, pp. 239-277.

— «La publicidad desleal: aproximación a la publicidad comparativa en su proyectada regulación en la Unión Europea», en La constitución española en el ordenamiento comunitario europeo (III): XVIII Jornadas de Estudio, 1999, pp. 565-612.

PEÑAS MOYANO, B. «La violación de normas concurrenciales y no concurrenciales como actos de competencia desleal», *Revista de Derecho de la Competencia y la Distribución*, núm. 3, 2008.

PETKOVA, B. y BOEHM, F. «Profiling and the Essence of the Right to Data Protection» in SELINGER, E., POLONETSKY, J. y TENE, O., *The Cambridge Handbook of Consumer Privacy,* Cambridge University Press, 2018, pp. 185-300.

PEUKERT, A., HUSOVEC, M., KRETSCHMER, M., MEZEI, P. y QUINTAIS, J. P., EUROPEAN COPYRIGHT SOCIETY. «Comment on Copyright and the Digital Services Act Proposal», *IIC – International Review of Intellectual Property and Competition Law*, 53(3), 2022.

PILA, J. y TORREMANS, P. L. C. «The law of copyright and related rights», en PILA, J. y TORREMANS, P. L. C., European Intellectual Property Law, Oxford, 2019, pp. 295-300.

PODSZUN, R. *Digital Markets Act: Article-by-Article Commentary*, Bloomsbury Publishing, 2024.

PRESTON, I. L. «Reasonable consumer or ignorant consumer? How the FTC decides», *Journal of Consumer Affairs*, 1974, pp. 248-270.

PRUNKL, C. «Human autonomy in the age of artificial intelligence», *Nature Machine Intelligence*, 2022, vol. 4, núm. 2.

PURNHAGEN, K. «More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?», en European Journal of Risk Regulation, vol. 8, núm. 2, 2017, pp. 437-440.

PURTOVA, N. «From Knowing by Name to Personalisation: Meaning of Identification Under the GDPR», *SSRN Electronic Journal*, 2021.

REBOLLO DELGADO, L. «Las condiciones de tratamiento de categorías especiales de datos (comentario al artículo 9 RGPD y al artículo 9 LOPDGDD)», en TRONCOSO REIGADA, A., *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, Tomo I, Aranzadi, 2021, pp. 1013-1039.

ROBLES MARTÍN-LABORDA, A. «Cuando el cartelista es un robot. Colusión en mercados digitales mediante algoritmos de precios», *Actas de Derecho Industrial y Derecho de Autor*, 2018.

RODILLA MARTÍ, C. «Los mercados de plataformas digitales: entre el Derecho de la competencia y la regulación», Revista General de Derecho de los Sectores Regulados: RSR, núm. 8, 2021.

— «Problemas de defensa de la competencia en el mercado de la publicidad online», en *Tax legal advisory review: La revista para el mundo económico-empresarial*, núm. 3, 2022, pp. 23-25.

Rodríguez Escanciano, S. y Gómez García, F. X. «La edad como factor de vulnerabilidad social: algunos factores merecedores de preocupación», *Derecho de las relaciones laborales*, 5, 2018.

Roffarello, A. y Russis, L. «Towards understanding the dark patterns that steal our attention» in *CHI EA '22: Extended abstracts of the 2022 CHI conference on human factors in computing systems,* 2022.

Romeo Casabona, C. M. «Datos genéticos (comentario al artículo 4.13 RGPD)», en Troncoso Reigada, A., *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales,* Tomo I, Aranzadi, 2021, pp. 697-707.

— «Datos relativos a la salud (comentario al artículo 4.15 RGPD)», en Troncoso Reigada, A., *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales,* Tomo I, Aranzadi, 2021, pp. 715-731.

Rubio Bravo, M.ª P. «Tecnologías de reconocimiento facial en las actuaciones previas al procedimiento administrativo sancionador: a propósito del asunto Glukhin c. Rusia», Revista española de derecho administrativo, núm. 237, 2024.

Ruiz Peris, J. I. «The EU Digital Markets Act, a European answer to application's problems of classical competition law to Gatekeepers», en Ruiz Peris, J. I. (dir.), *Competencia, compensación de daños y mercados digitales*, 2022, pp. 17-53.

Saas, R. «Manipulation, Algorithm Design, and the Multiple Dimensions of Autonomy». *Philos. Technol, Philos*, 37, 2024.

Sánchez Frías, A. *Los conceptos autónomos en el Derecho de la Unión Europea*, Tirant lo Blanch, 2023.

Sánchez Frías, I. «El marketing algorítmico basado en datos reveladores de un trastorno por uso de videojuegos: un análisis desde el Derecho de la Competencia desleal», en Tato Plaza, A.; Costas Comesaña, J.; Fernández Carballo-Calero, P.; Torres Pérez, F.; Louredo Casado, S. (dirs.), *Nuevas tendencias en el Derecho de la Competencia y de la Propiedad Industrial e Intelectual IV*, Tirant lo Blanch, 2024, pp. 533-567.

— «La prohibición de presentar publicidad basada en perfiles utilizando categorías especiales de datos en la Ley de Servicios Digitales. ¿A quién deja atrás? Especial referencia al dilema *pay-or-okay*», *Actas de derecho industrial y derecho de autor*, tomo 44, 2024.

— «Secondary uses of health data under the European Health Data Space: connections with the GDPR and the impact of AI», *Revista General de Derecho Europeo,* núm. 65, 2025.

Sánchez Solé, S. «La violación de normas como acto de competencia desleal. [Comentario a la Sentencia de la Audiencia Provincial de Valencia (Sección 6.ª) de 21 de marzo de 1994]», *RGD*, núm. 604-5, 1995.

Santos, C. *et al.,* «Which Online Platforms and Dark patterns should be regulated under article 25 of the DSA?», *SSRN Electronic Journal,* 2024.

Savin, A. «Profiling in the Present and New EU Data Protection Frameworks», en Nielsen, P. A., Schmidt, P. K., Dyppel Weber, K., *Erhvervsretlige emne, Juridisk Institut CBS,* Djøf Forlag, 2015, pp. 249-270.

Schricker, G. «Situación actual y evolución del derecho de la publicidad en la República Federal de Alemania», en Lema Devesa, C. (dir.), *Problemas actuales del derecho de la publicidad: Primeras Jornadas Internacionales de Derecho de la Publicidad*, Instituto Nacional de Publicidad, 1984.

Sears, A. M. «The Limits of Online Price Discrimination in Europe», *Science and Technology Law Review*, 21(1), 2021.

Senftleben, M. «Trademark Law, AI-Driven Behavioural Advertising and the Digital Services Act – Towards Source and Parameter Transparency for Consumers, Brand Owners and Competitors» in CHELTENHAM, *Research Handbook on Intellectual Property and Artificial Intelligence*, Edward Elgar, 2022.

Solove, D. J. «Data is what data does; regulating based on harm and risk instead of sensitive data», *Northwestern University Law Review*, vol. 118, núm. 4, 2024.

Soriano Arnanz, A. «Discriminación algorítmica: garantías y protección jurídica», en Cotino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, 2022, pp. 139-166.

Sotelo, F. «Candy Crush Saga: El secreto de un modelo de negocio de éxito», *Marketing for eCommerce*, 29 de septiembre de 2015.

Sousa E Silva, N. «The Artificial Intelligence Act: Critical Overview», *SSRN Electronic Journal*, 2024.

Speicher, T. *et al.,* «Potential for Discrimination in Online Targeted Advertising», *Journal of Machine Learning Research*, 2018.

Splinder, G. y Schmechel, P. «Datos personales y cifrado en el Reglamento General Europeo de Protección de Datos», *JIPITEC – Revista de Derecho de la Propiedad Intelectual, Tecnologías de la Información y Comercio Electrónico*, 7, 2016.

Stuyck, J. «The Court of Justice and the Unfair Commercial Practices Directive», *Common Market Law Review*, vol. 52, núm. 3, 2015, pp. 721-752.

— «The Notion of the Empowered and Informed Consumer in Consumer Policy and How to Protect the Vulnerable Under Such a Regime», en *The Yearbook of Consumer Law 2007*, 1.ª ed., Routledge, 2007, pp. 19-20.

Sumer, B. «When do the images of biometric characteristics qualify as special categories of data under the GDPR?: a systemic approach to biometric data processing», *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2022.

Susser, D. *et al.,* «Online Manipulation: Hidden Influences in a Digital World», *Georgetown Law Technology Review,* 2019.

Tapia Hermida, F. J. «El "consumidor medio", los sesgos cognitivos y las prácticas comerciales desleales de venta cruzada de préstamos y seguros», *La leyUnión Europea*, núm. 131, Sección Sentencias seleccionadas, 2024.

Tato Plaza, A. «Aspectos jurídicos de la publicidad a través de líderes de opinión en redes sociales ("influencers")», *Revista de Derecho Mercantil,* 2019.

— «La reforma de la Ley General de Publicidad», Revista de derecho de la competencia y la distribución, núm. 7, 2010, pp. 141-154.

— «Líneas generales de la reforma del derecho español contra la competencia desleal (Parte II)», *Autocontrol,* núm. 150, 2010, pp. 9-14.
— «Líneas generales de la reforma del derecho español contra la competencia desleal (Parte I)», *Autocontrol*, núm. 149, 2010, pp. 7-14.
— «Obligaciones específicas de información, engaño por omisión y principio de integridad de la campaña publicitaria», en Actas de derecho industrial y derecho de autor, tomo 38, 2017-2018.
— «Una primera aproximación al régimen jurídico de las prácticas agresivas en la Directiva sobre prácticas desleales con los consumidores», *Actas de Derecho Industrial y Derecho de Autor*, vol. 27, 2006-2007.
Tato Plaza, A. *et al.,* «Introducción», en Tato Plaza, A., Fernández Carballo-Calero, P. y Herrera Petrus, C., L*a reforma de la ley de competencia desleal*, La Ley Wolters Kluwer, 2010, pp. 29-57.
Tato Plaza, A. *et al.,* «La nueva cláusula general de represión de la competencia desleal», en Tato Plaza, A., Fernández Carballo-Calero, P. y Herrera Petrus, C., *La reforma de la ley de competencia desleal,* La Ley Wolters Kluwer, 2010, pp. 61-97.
Tato Plaza, A. *et al.,* «Prácticas agresivas», en Tato Plaza, A., Fernández Carballo-Calero, P. y Herrera Petrus, C., *La reforma de la ley de competencia desleal,* La Ley Wolters Kluwer, 2010, pp. 181-202.
Tato Plaza, A., Fernández Carballo-Calero, P. y Herrera Petrus, C., *La reforma de la ley de competencia desleal*, La Ley Wolters Kluwer, 2010.
Ter Laak, J. «Las cinco grandes dimensiones de la personalidad», *Revista de Psicología de la PUCP*, vol. xiv, N° 2, 1996.
Tomassi, S. «Digital Services and algorithmic discrimination», en *The risk of discrimination in the Digital Market. From the Digital Services Act to the future*, Springer, 2022, pp. 37-54.
Trzaskowski, J. «Persuasion, Manipulation, Choice Architecture and 'Dark Patterns'», en Savin, A.; Trzaskowski, J. (eds.), Research Handbook on EU Internet Law, 2.ª ed., Edward Elgar, 2023, pp. 325-328.
Valcke, P., Clifford, D. y Dessers, V., «Constitutional Challenges in the Emotional AI Era», en Micklitz, H. W. *et al.*, *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2021, pp. 57-77.
Van Eijk, N., Jay Hoofnagle, C. y Kannekens, E. «Unfair Commercial Practices: A Complementary Approach to Privacy Protection», *European Data Protection Law Review*, 3(3), 2017.
Vardhan, J. V., Kalyan Chakravarti, Y. y Chand, A. J. «Emotion Recognition by Facial Expressions and Speech Using Deep Learning», *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 2024.
Vargas Marcos, F. «La contaminación ambiental como factor determinante de la salud», *Revista española de salud pública*, 2005.
Vázquez Ruano, T. «Aproximación jurídica al spam desde la protección de datos de carácter personal», Revista de la contratación electrónica, núm. 33, 2002.
— «El spam y la nueva regulación de la Ley de Competencia Desleal», Revista de Derecho Mercantil, núm. 277, 2010.
Vega Vega, J. A. «Artículo 32. Acciones», en Bercovitz Rodríguez-Cano, A. (dir.), *Comentarios a la Ley de Competencia Desleal*, 2011, Aranzadi, pp. 847-887.

Vivero de Porras, C. «Publicidad ilícita por vía electrónica como acto de competencia desleal: publicidad personalizada en Instagram», *Actas de Derecho Industrial,* 2023, pp. 57-80.

Voigt, P. y Von Dem Bussche, A. *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, 2017.

Wachter, S., Mittelstadt, B. «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbia Business Law Review*, 2019.

Wachter, S., «Affinity profiling and discrimination by association in *online* behavioral advertising», *Berkeley Technology Law Journal*, vol. 35, núm. 2, 2020.

Wang, H. J., Yue, X. L., Ansari, A. R., Tang, G. Q., Ding, J. Y. y Jiang, Y. Q. «Research on the Influence Mechanism of Consumers' Perceived Risk on the Advertising Avoidance Behavior of Online Targeted Advertising», *Front Psychol,* 2022.

Wang, Y. «Do not go gentle into that good night: The European Union's and China's different approaches to the extraterritorial application of artificial intelligence laws and regulations», *Computer Law & Security Review*, vol. 53, 2024.

Warren, S. D. y Brandeis, L. D. «The Right to Privacy», *Harvard Law Review,* vol. 4, 1890.

Wendehorst, C. «Of elephants in the room and paper tigers: how to reconcile data protection in data economy», en Lohsse, S., Schulze, R. y Staudenmayer, D. *Trading data in the digital economy: legal concepts and tools*, Nomos, 2017, pp. 327-357.

Wiedemann, K. «Profiling and (automated) decision-making under the GDPR: A two-step approach», *Computer Law & Security Review*, 45, 2022.

Zanfir-Fortuna, G. «Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package», *EDPS at 20 Anniversary Volume*, 2024.

Zarsky, T. Z., «Privacy and Manipulation in the Digital Age», *Theoretical Inquiries in Law*, vol. 20, 2019.

Zimmer, D. «Property rights regarding data?», en Lohsse, S., Schulze, R. y Staudenmayer, D., *Trading data in the digital economy: legal concepts and tools*, Nomos, 2017, pp. 101-133.

Zuboff, S. *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós, 2020.

2. Documentos oficiales, informes, artículos y entradas

AEPD, «Guía sobre tratamientos de control de presencia mediante sistemas biométricos», 2023.

— «IoT (I): Qué es IoT y cuáles son sus riesgos», 2020, disponible en *https://www.aepd.es/prensa-y-comunicacion/blog.*

— «Privacidad de grupo», 2020, disponible en *https://www.aepd.es/prensa-y-comunicacion/blog/privacidad-de-grupo.*

Amazon, «AI image generation», disponible en: *https://advertising.amazon.com/blog/ai-image-generation.*

Article 29 Data Protection Working Party, «Advice paper on special categories of data ("sensitive data")», 2011.
— «Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679», 2017.
— «Guidelines on the right to data portability», 2016.
Asociación de Medios de Información, «Los medios de información agrupados en AMI demandan a META por competencia desleal y reclaman más de 550 millones», 2023, disponible en: *https://www.ami.info/ami-demanda-a-meta-por-competencia-desleal-y-reclama-mas-de-550-millones.html.*
Balado, L. «¿Buscas tus síntomas en Google? "El problema es que uno encuentra lo que quiere encontrar"», *La Voz de Galicia*, 2022.
Builtwith PTY LTD., «Google Analytics Usage Statistics», disponible en: *https://trends.builtwith.com/analytics/Google-Analytics*.
Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T.A. y Van Alstyne, M., *The EU Digital Markets Act: A Report from a Panel of Economic Experts*, Publications Office of the European Union, 2021.
CNIL, «Cookie walls: la CNIL publie des premiers critères d'évaluation», versión actualizada de 2022.
Comisión Europea, «Comunicación de la Comisión relativa a la definición de mercado de referencia a efectos de la normativa de la Unión en materia de competencia», *DOUE* núm. 1645, 2024, pp. 1-35.
— *Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE relativa a las prácticas comerciales desleales*, 2021.
— «La Comisión incoa un procedimiento formal contra Temu en virtud de la Ley de Servicios Digitales», 2024.
— «Libro Verde sobre Comunicaciones Comerciales en el Mercado Interior», 1997.
— *Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible*, 2020.
Competition and Markets Authority, *Online platforms and digital advertising Market study final report 1 July 2020*.
Council of Europe's Committee of Ministers, «Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes», 2019.
Council of the European Union, «Council position and findings on the application of the General Data Protection Regulation (GDPR), 15507/23», 2023.
Davidson, D., «Facebook Exploits 'Insecure' to Sell Ads», *The Australian*, 2017.
DCMS Committee, «Disinformation and 'fake news'», 2018.
Dischler, J., «Una nueva era de Google Ads impulsada por Inteligencia Artificial», 2023, disponible en *https://blog.google/intl/es-419/una-nueva-era-de-google-ads-impulsada-por-inteligencia-artificial/*
EDPB-EDPS, «Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)», 2021.
EDPB, «Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)».
— «Guidelines 3/2019 on processing of personal data through video devices», 2019.

— «Opinion 08/2024 on Valid Consent In The Context Of Consent Or Pay Models Implemented By Large Online Platforms», 2024.
EDPS, «Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative», 2023.
European Commission Press Corner, «Commission designates second set of Very Large Online Platforms under the Digital Services Act», 2023, disponible en *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763.*
European Commission, «AI Act Proposal explanatory memorandum», 2023.
— *Call for evidence: Digital fairness – fitness check on EU consumer law*, 2022.
— *Communication to the Commission. Approval of the content of the draft Communication from the Commission – Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, 2025.
— «DSA: Guidance on the requirement to publish user numbers», 2023.
— «Ethics Guidelines on Trustworthy AI», 2019.
— «Guidance Note on the collection and use of equality data based on racial or ethnic origin», *Publications Office*, 2021.
— «Political guidelines of the European Commission 2019-2024», disponible en *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_en.*
— «Preliminary Report – Sector Inquiry Into Consumer Internet Of Things», 2021.
European Commission, Directorate-General for Justice and Consumers, Farkas, L., «Analysis and comparative review of equality data collection practices in the European Union – Data collection in the field of ethnicity», *Publications Office*, 2017.
European Law Institute (ELI), «Guidelines on the Application of the Definition of an AI System in the AI Act: ELI Proposal for a Three-Factor Approach», 2024.
— «European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law. Response of the European Law Institute», 2023.
Feasey, R. y De Streel, A., «Data sharing for digital markets contestability: towards a governance framework», *CERRE Report*, 2020.
Google, «How Google Analytics works», *https://support.google.com/analytics/answer/12159447*.
— «Informe de transparencia. Retirada de contenido por infracciones de derechos de autor», 2024, disponible en *https://transparencyreport.google.com/*
— «Powered IA solutions», *https://ads.google.com/intl/es-419_ALL/home/campaigns/ai-powered-ad-solutions/*.
— «Usa la IA para generar código humano», *https://cloud.google.com/use-cases/ai-code-generation?hl=es*.
Grady, P. «EU's AI Act Resurrects Subliminal Messaging Panic», *Center for Data Innovation*, 2022, *https://datainnovation.org/2022/10/eus-ai-act-resurrects-subliminal-messaging-panic/*.
Graef, I. «Why end-user consent cannot keep markets contestable», *Verfassungs Blog*, 2021.

Grupo de Expertos de Alto Nivel Sobre la IA, «Directrices éticas para una inteligencia artificial fiable», Comisión Europea, 2018.

Grupo de Trabajo del Artículo 29 sobre Protección de Datos, «Dictamen 4/2007 sobre el concepto de datos personales», 2007.

— «Documento de trabajo sobre datos genéticos», 2004.

Hoffmann, L. J. «Fairness in the Digital Markets Act», *European Papers*, disponible en *https://www.europeanpapers.eu/en/europeanforum/fairness-in-digital-markets-act*.

Horowitz, A. H., Stickgold, R. y Zadra, A. «Inside your dreamscape», 2021, disponible en *https://aeon.co/essays/dreams-are-a-precious-resource-dont-let-advertisers-hack-them*.

Irish Council for Civil Liberties, «Greater protection in Article 5 (a) of the Commission's proposal for a Digital Markets Act», disponible en *https://www.iccl.ie/news/the-eu-digital-markets-act-requires-tighter-language/*

Irish Data Protection Commission, Decision of December 31, 2022, DPC Inquiry Reference: IN-18-5-5 y DPC Inquiry Reference: IN-18-5-7, disponible en *https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland*.

ISO/IEC 22989:2022, «Information technology — Artificial intelligence — Artificial intelligence concepts and terminology», 2022.

Krupiy, T. «Why the Proposed Artificial Intelligence Regulation Does Not Deliver on the Promise to Protect Individuals from Harm», *European Law Blog*, 2022, disponible en *https://www.europeanlawblog.eu/pub/why-the-proposed-artificial-intelligence-regulation-does-not-deliver-on-the-promise-to-protect-individuals-from-harm/release/1*.

Laux, J. «The shape of personalization to come», *Verfassungblog*, 2023.

Meta, «Business Ads Meta advantage», disponible en *https://en-gb.facebook.com/business/ads/meta-advantage.*

Observatorio de Trabajo, Algoritmo y Sociedad, «Adversarial Audit of ride-hailing platforms. Algorithmic compliance with competition, labor and consumer law in Spanish State», disponible en *https://eticas.ai/wp-content/uploads/2024/04/Adversarial-Audit-of-Rade-Hailing-Platforms.pdf*.

OECD, «Explanatory memorandum on the updated OECD definition of an AI system», *OECD Artificial Intelligence Papers,* núm. 8, OECD Publishing, 2024.

Oliveira Hashiguchi, T. C., Slawomirski, L. y Oderkirk, J. «Laying the foundations for artificial intelligence in health», *OECD Health Working Papers*, núm. 128, disponible en *https://www.oecd.org/en/publications/laying-the-foundations-for-artificial-intelligence-in-health_3f62817d-en.html*.

Organización Mundial de la Salud, CIE-11. *Clasificación Internacional de Enfermedades, 11.a revisión. Estandarización mundial de la información de diagnóstico en el ámbito de la salud.*

Ovington, R. y Lewis, D., «Virtual assistants and the DMA», 2022, disponible en *https://www.frontier-economics.com/uk/en/news-and-insights/articles/article-i9498-virtual-assistants-and-the-dma/*

Parris, T. y Angwin J. «Facebook lets advertisers exclude users by race», *ProPublica,* 2016, disponible en *https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.*

Perrigo, B. «"The Capabilities Are Still There". Why Cambridge Analytica Whistleblower Christopher Wylie Is Still Worried», *TIME*, 2019, disponible en *https://time.com/5695252/christopher-wylie-cambridge-analytica-book.*

Poullet, Y. y Dinant, J. M., «Report on The Application of Data Protection Principles to the Worldwide Telecommunication Networks: Information Self-Determination in The Internet Era: Thoughts on Convention For The Purposes Of The Future Work Of The Consultative Committee», núm. 108, 2004.

Reyna, A. «Why the DMA is much more than competition law (and should not be treated as such)», disponible en: *https://chillingcompetition.com/2021/06/16/why-the-dma-is-much-more-than-competition-law-and-should-not-be-treated-as-such-by-agustin-reyna.*

Sherman, L., «Uber's New Math: Increase Prices And Squeeze Driver Pay», Forbes, 2023, disponible en *https://www.forbes.com/sites/lensherman/2023/01/16/ubers-new-math-increase-prices-and-squeeze-driver-pay/#:~:text=Armed%20with%20such%20market%20insight,their%20known%20willingness%20to%20serve*.

The Brussels Time, «Uber fares allegedly linked to phone battery levels», 2024, disponible en *https://www.brusselstimes.com/449143/uber-fares-allegedly-linked-to-phone-battery-levels.*

Whittle, M. *et al.*, *Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161*, European Commission, 2024.

World Health Organization, «Gender and Health», disponible en *https://www.who.int/health-topics/gender#tab=tab_1.*

Zuiderveen, B. «Discrimination, artificial intelligence and algorithmic decision-making», *Council of Europe, Directorate General of Democracy*.

3. NORMATIVA

3.1. *Internacional y de la Unión Europea*

Carta de los Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000. Diario Oficial de las Comunidades Europeas (2000/C 364/01) (cit. La Carta).

Convenio Europeo sobre Televisión Transfronteriza, Serie de Tratados Europeos, núm. 132, de 5 de mayo de 1989.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información (cit. CDSMD).

Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) núm. 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales»).

Directiva 2006/114/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, sobre publicidad engañosa y publicidad comparativa.

Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997.

Propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, cit. RGPD).

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE.

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 (cit. P2B).

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, cit. DMA).

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, cit. DSA).

Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo (Reglamento de Máquinas).

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) núm. 300/2008, (UE) núm. 167/2013, (UE) núm. 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 (Reglamento de Inteligencia Artificial).
Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política.
Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847.
Tratado de Funcionamiento de la Unión Europea, de 13 de diciembre de 2007, versión consolidada (cit. TFUE).

3.2. *Española*

Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978.
Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil (cit. CC).
Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
Ley 20/2011, de 21 de julio, del Registro Civil.
Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (cit. LECiv).
Ley 3/1991, de 10 de enero, de Competencia Desleal (cit. LCD).
Ley 34/1988, de 11 de noviembre, General de Publicidad (cit. LGP).
Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

3.3. *Terceros países*

Código belga de Derecho Económico (*Code de droit Économique*).
Decreto francés núm. 92-280 de 27 de marzo de 1992 relativo a la publicidad y patrocinio audiovisual (*Décret n° 92-280 du 27 mars 1992 relatif à la publicité et au parrainage audiovisuels*).
Decreto Legislativo italiano de 2 de agosto de 2007, núm. 145/2007 (*Decreto Legislativo 2 agosto 2007, núm. 145, Attuazione dell'articolo 14 della direttiva 2005/29/CE che modifica la direttiva 84/450/CEE sulla pubblicità ingannevole*).
Decreto Legislativo italiano de 25 de enero de 1992, núm. 74 (*Decreto Legislativo 25 gennaio 1992, núm. 74, Attuazione della direttiva 84/450/CEE, come modificata dalla direttiva 97/55/CE in materia di pubblicità ingannevole e comparativa*).
Ley alemana contra la competencia desleal (*Gesetz gegen den unlauteren Wettbewerb)* (cit. UWG).
Ley de Defensa de la Competencia alemana (Gesetz gegen Wettbewerbsbeschränkungen, cit. GWB).
Ley danesa de Prácticas de Comercialización (*Bekendtgørelse af lov om markedsføring*).
Ley de la República de Irlanda de Protección del Consumidor de 2007 (*Consumer Protection Act 2007*).

Ley de Privacidad de Connecticut (*Connecticut Data Privacy Act of 2023, «CTDPA»)*.
Ley de Privacidad del Consumidor de California (*California Consumer Privacy Act of 2018*, *«CCPA»)*.
Ley Federal austríaca contra la Competencia Desleal (*Bundesgesetz gegen den unlauteren Wettbewerb)*.
Ley griega núm. 2251/1994 de Protección del Consumidor (Νόμος 2251/1994, Προστασία των καταναλωτών).
Ley sueca de Comercialización (*Marknadsföringslagen*).

4. JURISPRUDENCIA

4.1. *Unión Europea*

Sentencia del Tribunal de Justicia de la Unión Europea, de 20 de febrero de 1979, *Rewe-Zentral AG contra Bundesmonopolverwaltung für Branntwein (Cassis de Dijon)*, asunto C-120/78 (ECLI:EU:C:1979:42).
Sentencia del Tribunal de Justicia de la Unión Europea, de 26 de junio de 1997, *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH contra Heinrich Bauer Verlag*, asunto C-368/95 (ECLI:EU:C:1997:325).
Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 1998, *Gut Springenheide GmbH y Rudolf Tusky contra Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung*, asunto C-210/96 (ECLI:EU:C:1998:369).
Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de enero de 2000, *Estée Lauder Cosmetics GmbH & Co. OHG contra Lancaster Group GmbH*, asunto C-220/98 (ECLI:EU:C:2000:8).
Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de septiembre de 2000, *Adolf Darbo AG contra Bundesminister für soziale Sicherheit und Generationen*, asunto C-465/98 (ECLI:EU:C:2000:184).
Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de abril de 2000, *Verein gegen Unwesen in Handel und Gewerbe Köln eV contra Adolf Darbo AG*, asunto C-465/98 (ECLI:EU:C:2000:184).
Sentencia del Tribunal de Justicia de la Unión Europea, de 20 de mayo de 2003, *Rechnungshof v Österreichischer Rundfunk y otros* (casos acumulados C-465/00, C-138/01 y C-139/01; Christa Neukomm y Joseph Lauermann v Österreichischer Rundfunk), asunto C-465/00 (ECLI:EU:C:2003:294). Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, *Bodil Lindqvist,* asunto C-101/01 (ECLI:EU:C:2003:596).
Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de septiembre de 2004, *Waddenvereniging y Vogelbeschermingsvereniging,* asunto C-127/02 (ECLI:EU:C:2004:482).
Sentencia del Tribunal de Justicia de la Unión Europea, de 17 de julio de 2008*, S. Coleman contra Attridge Law y Steve Law*, asunto C-303/06 (ECLI:EU:C:2008:415).
Sentencia del Tribunal de Justicia de la Unión Europea, de 23 de abril de 2009, *VTB-VAB NV contra Total Belgium NV y Galatea BVBA contra*

Sanoma Magazines Belgium NV, asuntos acumulados C-261/07 y C-299/07 (ECLI:EU:C:2009:244).

Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de enero de 2010, *Zentrale zur Bekämpfung unlauteren Wettbewerbs eV contra Plus Warenhandelsgesellschaft mbH*, asunto C-304/08 (ECLI:EU:C:2010:12).

Sentencia del Tribunal de Justicia de la Unión Europea, de 9 de noviembre de 2010, *Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG contra «Österreich»-Zeitungsverlag GmbH*, asunto C-540/08 (ECLI:EU:C:2010:660).

Sentencia del Tribunal de Justicia de la Unión Europea, de 26 de abril de 2012, *Nemzeti Fogyasztóvédelmi Hatóság contra Invitel Távközlési Zrt*, asunto C-472/10 (ECLI:EU:C:2012:242).

Sentencia del Tribunal de Justicia de la Unión Europea, de 18 de octubre de 2012, *Purely Creative Ltd y otros contra Office of Fair Trading,* asunto C-428/11 (ECLI:EU:C:2012:651).

Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de marzo de 2013, *Euronics Belgium CVBA contra Kamera Express BV y Kamera Express Belgium BVBA*, asunto C-343/12 (ECLI:EU:C:2013:154).

Sentencia del Tribunal de Justicia de la Unión Europea, de 11 de abril de 2013, *Peter Sweetman y otros contra An Bord Pleanála,* asunto C-258/11 (ECLI:EU:C:2013:220).

Sentencia del Tribunal de Justicia de la Unión Europea, de 18 de julio de 2013, *Citroën Belux NV contra Federatie voor Verzekerings- en Financiële Tussenpersonen (FvF),* asunto C-265/12 (ECLI:EU:C:2013:498).

Sentencia del Tribunal de Justicia de la Unión Europea, de 19 de septiembre de 2013, *CHS Tour Services GmbH contra Team4 Travel GmbH,* asunto C-435/11 (ECLI:EU:C:2013:574).

Sentencia del Tribunal de Justicia de la Unión Europea, de 3 de octubre de 2013, *BKK Mobil Oil Körperschaft des öffentlichen Rechts contra Zentrale zur Bekämpfung unlauteren Wettbewerbs eV,* asunto C-59/12 (ECLI:EU:C:2013:634).

Sentencia del Tribunal de Justicia de la Unión Europea, de 19 de diciembre de 2013, *Trento Sviluppo Srl y Centrale Adriatica Soc. Coop. Arl contra Autorità Garante della Concorrenza e del Mercato,* asunto C-281/12 (ECLI:EU:C:2013:859).

Sentencia del Tribunal de Justicia de la Unión Europea, de 19 de marzo de 2015, *E.ON Földgáz Trade Zrt v Magyar Energetikai és Közmű-szabályozási Hivatal,* asunto C-510/13 (ECLI:EU:C:2015:189).

Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de junio de 2015, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. contra Teekanne GmbH & Co. KG,* asunto C-195/14 (ECLI:EU:C:2015:361).

Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2015, *CHEZ Razpredelenie Bulgaria AD contra Komisia za zashtita ot diskriminatsia,* asunto C-83/14 (ECLI:EU:C:2015:480).

Sentencia del Tribunal de Justicia de la Unión Europea, de 12 de junio de 2019, *Prezes Urzędu Ochrony Konkurencji i Konsumentów contra Orange Polska S.A.,* asunto C-628/17 (ECLI:EU:C:2019:480).

Sentencia del Tribunal de Justicia de la Unión Europea, de 25 de noviembre de 2021, *StWL Städtische Werke Lauf a.d. Pegnitz GmbH y eprimo GmbH*, asunto C-102/20 (ECLI:EU:C:2021:954).
Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de agosto de 2022, *OT y Vyriausioji tarnybinės etikos komisija,* asunto C-184/20 (ECLI:EU:C:2022:601).
Sentencia del Tribunal General de la Unión Europea, de 26 de abril de 2023, asunto T-557/20, Junta Única de Resolución y Supervisor Europeo de Protección de Datos (ECLI:EU:T:2023:219).
Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de julio de 2023, *Meta Platforms y Bundeskartellamt,* asunto C-252/21 (ECLI:EU:C:2023:537).
Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de diciembre de 2023, *OQ contra Land Hessen*, asunto C-634/21 (ECLI:EU:C:2023:957).
Sentencia del Tribunal de Justicia de la Unión Europea, de 4 de octubre de 2024, *Winthir Apotheke v Lindenapotheke*, asunto C-21/23 (ECLI:EU:C:2024:846).
Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de noviembre de 2024, *Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato*, asunto C-646/22 (ECLI:EU:C:2024:957).

4.2. *España*

STS de 13 de marzo de 2000 [RJ 2000, 1207].
STS de 29 de marzo de 2001 [RJ 2001, 3189].
STS de 29 de diciembre de 2006 [RJ 2007, 1714].
STS de 23 de marzo de 2007 [RJ 2007, 8095].
SAP de Castellón [Secc. 3.ª] de 10 de octubre de 2007 [JUR 2008, 119897].
STS de 5 de febrero de 2008 [RJ 2008, 4029].
SAP de Granada [Secc. 3.ª] de 15 de febrero de 2008 [JUR 2008, 333027].
SAP de Barcelona [Secc. 3.ª] de 11 de marzo de 2008 [EDJ 144196].
SAP de Tarragona [Secc. 1.ª] de 25 de marzo de 2008 [JUR 2008, 207190].
SAP de Madrid [Secc. 20.ª] de 7 de mayo de 2008 [JUR 2008, 333027].
STS de 17 de julio de 2008 [RJ 2008, 4482].
STS de 2 de marzo de 2009 [RJ 2009, 2789].
Sentencia del Juzgado de lo Mercantil núm. 1 de Zaragoza núm. 19/2014, de 23 de enero [TOL 5581452].
Sentencia del Juzgado de lo Mercantil núm. 3 de Barcelona de 2 de mayo de 2017 [TOL 6215639].
SAP de Barcelona [Secc. 15.ª] de 15 de noviembre de 2018 [TOL 7559780].
STS de 3 de octubre de 2019 [RJ 2018, 1748].
SAP de Madrid [14.ª] núm. 100/2019, de 20 de marzo [TOL 7314998].

4.3. *Alemania*

Sentencia del Tribunal de Primera Instancia de Berlín, de 27 de marzo de 2007-5 C 314/06.
Sentencia del Tribunal de Primera Instancia de Múnich, de 30 de septiembre de 2008-133 C 5677/08.

Sentencia del Tribunal de lo Contencioso-Administrativo de Wiesbaden, de 27 de febrero de 2009-6 K 1045/08.WI.
Sentencia del Tribunal de Distrito de Wuppertal, de 19 de octubre de 2010-25 Qs 10 Js 1977/08-177/10.
Sentencia del Tribunal de Primera Instancia de Berlín, de 31 de enero de 2013-57 S 87/08.

4.4. *Francia*

Sentencia del Tribunal de Apelación de París, de 15 de mayo de 2007 – Henri S. c. SCPP.

4.5. *Reino Unido*

Tribunal Superior de Inglaterra y Gales (Tribunal Administrativo), [2011] EWHC 1430 (Admin), Caso No. CO/12544/2009.
Tribunal Superior (Sala de lo Contencioso-Administrativo de Apelaciones), [2011] UKUT 153 (AAC), número de recurso: GI/150/2011, GI/151/2011, GI/152/2011.

ISBN: 979-13-87913-49-6

La personalización de la publicidad y de otras prácticas comerciales mediante sistemas de inteligencia artificial ofrece indudables ventajas, pero también permite explotar datos sensibles y situaciones de vulnerabilidad con un gran nivel de precisión.

Esta obra analiza críticamente la respuesta del Derecho nacional y del Derecho de la Unión Europea frente a estas prácticas. Examina las interacciones entre el Reglamento General de Protección de Datos, el Reglamento de Servicios Digitales, el Reglamento de Mercados Digitales, el Reglamento de Inteligencia Artificial y la normativa sobre prácticas comerciales desleales, así como los conflictos, lagunas y dificultades interpretativas que plantea su aplicación conjunta.

El estudio presta especial atención a la publicidad basada en perfiles, la explotación comercial de vulnerabilidades, las prácticas manipuladoras o subliminales y el papel de la competencia desleal como mecanismo de tutela, ofreciendo propuestas interpretativas para afrontar los nuevos riesgos de la personalización en los mercados digitales.

Marcial Pons