ADI 44 (2024): 407-421

LA PROHIBICIÓN DE PRESENTAR PUBLICIDAD BASADA EN PERFILES UTILIZANDO CATEGORIAS ESPECIALES DE DATOS EN LA LEY DE SERVICIOS DIGITALES. ¿A QUIÉN DEJA ATRÁS? ESPECIAL REFERENCIA AL DILEMA *PAY-OR-OKAY*

THE DIGITAL SERVICES ACT´S BAN ON PRESENTING ADVERTISING BASED ON PROFILING USING SPECIAL CATEGORIES OF DATA. WHO IS LEFT BEHIND? A PARTICULAR EMPHASIS ON THE PAY-OR-OKAY CONUNDRUM

Irene Sánchez Frías*

RESUMEN

Con el auge de complejos sistemas de IA, el análisis masivo de datos sensibles ha permitido el desarrollo de prácticas publicitarias que pueden producir efectos adversos para los destinatarios de comunicaciones comerciales. La creciente materialización de estos efectos ha llevado al legislador comunitario a incluir una prohibición en el Reglamento de Servicios Digitales que impide a los prestadores de servicios de plataforma presentar publicidad basada en la elaboración de perfiles utilizando datos sensibles. El presente trabajo analiza los principales déficits de la prohibición, prestando especial atención al modelo ***pay-or-okay*** como particular ejemplo de la inseguridad jurídica que rodea la actual normativa de protección de datos, la cual resulta de aplicación en aquellos casos no cubiertos por la nueva prohibición. El objetivo principal del trabajo es evidenciar las lagunas de la prohibición y proponer posibles soluciones, ***de lege lata*** y de ***lege ferenda,*** para paliar las mismas.

Palabras clave: Publicidad basada en la elaboración de perfiles, datos sensibles, plataformas en línea, guardianes de acceso, modelo ***pay-or-okay***, Reglamento General de Protección de Datos, Ley de Servicios Digitales, Ley de Mercados Digitales.

* Investigadora predoctoral FPU en Derecho mercantil, Universidad de Málaga. Graduada en el Master Avanzado en Propiedad Intelectual y Derecho de las TIC, Universidad Católica de Lovaina (KU Leuven). Este trabajo se ha desarrollado en el marco de las actividades del Proyecto de Investigación CODIG-IA «Marco Jurídico Para La Competencia Dinámica En Mercados Digitales Y Para La Innovación A Través De Inteligencia Artificial» (PID2021-122536OB-I00), financiado por el Ministerio de Ciencia, Innovación y Universidades, (IP Eugenio Olmedo Peralta), así como en el Proyecto Andaluz de Investigación CoMeDi "Consumidores y pequeños profesionales en la contratación en Mercados Digitales: prácticas anticompetitivas, desleales y explotación de dependencia económica (ProyExcel_00665 PAIDI 2020), (IPs: Eugenio Olmedo Peralta y Patricia Benavides Velasco). Correo electrónico: *irenesanchezfrias@uma.es*.

Fecha de recepción: 31 de marzo de 2024 // Fecha de aceptación: 21 de mayo de 2024.

ABSTRACT

With the rise of complex AI systems, the massive analysis of sensitive data has enabled the development of advertising practices that may have adverse effects on the recipients of commercial communications. The increasing materialisation of these effects has led the EU legislator to include a prohibition in the Digital Services Regulation that prevents platform service providers from presenting advertising based on profiling using sensitive data. This paper analyses the main shortcomings of the ban, with special consideration of the pay-or-okay model as a particular example of the legal uncertainty surrounding the current data protection legislative framework, which applies in those cases not covered by the new ban. The main objective of the paper is to highlight the loopholes of the prohibition and to propose possible solutions, ***de lege lata*** and ***de lege ferenda***, to remedy them.

Keywords: Advertising based on profiling, sensitive data, online platforms, gatekeepers, pay-or-okay systems, General Data Protection Regulation, Digital Services Act, Digital Markets Act.

I. PRELIMINAR

La regulación de los datos sensibles, denominados bajo el RGPD «Categorías Especiales De Datos», se formuló como un desafío desde su propio nacimiento, abarcando una miríada de dilemas que no han hecho sino extenderse en los últimos años[1][2]. Con el paso de los años, datos que originalmente no se consideraron sensibles —como la situación financiera de un individuo[3]— comienzan a producir efectos discriminatorios graves[4], planteando la cuestión de si debieran quedar sometidos al mismo régimen jurídico. De igual forma, la evolución de complejos sistemas algorítmicos ha permitido, a través del análisis masivo de datos aisladamente no sensibles, que se infieran conclusiones que sí lo son, como la orientación sexual o la raza[5].

---

[1] Bajo la categoría de datos sensibles —denominados categorías especiales de datos— el art. 9.1. del RGPD se refiere exclusivamente a 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».

[2] Malgieri (2020), págs. 1583-1612.

[3] Collado-Rodríguez (2021), págs. 41–67.

[4] Kamiran (2013), versión online.

[5] Wachter (2020), págs. 369-392.

La posibilidad de micro segmentar a la población mediante el análisis de Big Data guarda un especial papel en la publicidad en línea, cada vez más basada en la elaboración de perfiles por su alto nivel de efectividad y por sus evidentes beneficios, entre otros, la capacidad de filtrar los contenidos que nos interesan entre el exceso de información digital en la que vivimos[6]. Sin embargo, también entraña riesgos significativos, como la presentación de anuncios que afecten a la igualdad de trato y a las oportunidades de los destinatarios, o la manipulación de la capacidad para la toma de decisiones comerciales[7]. Consciente de estos riesgos, el legislador comunitario ha decidido abordar de forma específica esta problemática. El Reglamento de Servicios Digitales[8] introduce en su art. 26.3 una nueva prohibición en el marco legislativo de la UE, al establecer que los prestadores de plataformas en línea no presentarán a los destinatarios anuncios basados en la elaboración de perfiles utilizando datos sensibles. Abordaremos en estas páginas los problemas jurídicos que entraña la aplicación de esta prohibición.

II. ÁMBITO MATERIAL. LA PROHIBICIÓN DE PRESENTAR PUBLICIDAD BASADA EN LA ELABORACIÓN DE PERFILES UTILIZANDO DATOS SENSIBLES

Para identificar las principales carencias de la prohibición, es necesario comenzar analizando qué actividad queda prohibida bajo la misma y, por exclusión, qué acciones relacionadas están permitidas, aun con ciertos matices. Bajo el art. 26.3 de la DSA, la actividad que queda prohibida es «Presentar» publicidad en línea basada en la elaboración de perfiles utilizando datos sensibles, dejando de lado otras prácticas en el ámbito publicitario, tales como el diseño de contenidos. Esta distinción pone de manifiesto que la prohibición se dirige principalmente a las plataformas que prestan servicios de publicidad, permitiendo a los anunciantes llegar a aquellos destinatarios que potencialmente pudieran estar más interesados en sus anuncios (*matching*), y ofreciendo su interfaz como espacio en el que se muestren los mensajes publicitarios[9]. Para cumplir con la prohibición, la plataforma deberá adaptar y monitorizar el sistema de toma de decisiones de su algoritmo publicitario, incluyendo qué datos de entrada se utilizan (y cuáles no) y qué proceso sigue el algoritmo para que el anuncio se dirija a un perfil y no a otro[10].

Para quedar sometida a la prohibición, la actividad publicitaria ha de presentar tres caracteres principales: i) debe caer dentro de la definición de «publicidad» a efectos de la DSA, ii) debe estar basada en la elaboración de perfiles y iii) deben haberse utilizado datos sensibles.

En cuanto al primer elemento, la DSA emplea una definición propia del concepto «publicidad», al señalar que es toda información destinada a promover el mensaje de una persona física o jurídica, independientemente de que se trate

---

[6] Castillo Parrilla (2023), págs. 53-88.

[7] Tzoulia (2021), págs. 447-477.

[8] 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 (DOUE-L-2022-81573). En adelante, «DSA», por sus siglas en inglés (Digital Services Act).

[9] AEDP, *Guía sobre el uso de cookies*, 2024.

[10] Edelson (2023), págs. 46-53.

de alcanzar fines comerciales o no comerciales, presentada por una plataforma en línea en su interfaz en línea a cambio de una remuneración específica por promover dicha información[11]. De forma más simple, cualquier mensaje presentado por una plataforma a cambio de una remuneración tendrá la consideración de publicidad a afectos de la norma. Resulta apreciable que el legislador comunitario ha querido optar por un concepto amplio de publicidad, ya que no se requiere siquiera un fin comercial, sino que basta con que la información se presente a cambio de una remuneración.

Para el segundo elemento, «elaboración de perfiles», la DSA se remite al RGPD, el cual define esta actividad como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física[12]. Siguiendo una interpretación contextual, entendemos que los perfiles comprendidos no son sólo los perfiles individuales, sino también los perfiles por afinidad a un grupo que conforman la base de la publicidad segmentada o por categorías[13]. Esta interpretación se deriva de los propios considerandos de la DSA[14], al señalar que se prohíbe presentar anuncios i) basados en la elaboración de perfiles utilizando datos sensibles (perfiles individuales) o ii) basados en la elaboración de perfiles basados en categorías de perfiles que usen datos sensibles (perfiles por segmentación o afinidad a un grupo).

El tercer elemento que compone la publicidad vetada por la DSA radica en que para la elaboración de perfiles publicitarios se deben haber utilizado datos sensibles, para cuya definición la DSA también se remite al RGPD[15]. Ello conduce a la primera gran laguna que presenta la prohibición. Inicialmente, podríamos interpretar que el ámbito material de la prohibición es bastante extenso, dado el carácter amplio de la definición de «publicidad» y de «elaboración de perfiles». Sin embargo, la prohibición se acota a «presentar» publicidad basada en la elaboración de perfiles utilizando datos sensibles, pero nada dice del tratamiento de estos datos sensibles, que es donde surge la raíz del problema. Al remitirse al RGPD en todo lo referente al tratamiento de datos personales, la DSA hereda íntegramente el conjunto de carencias que presenta la regulación de los datos sensibles desde hace varios años. Entre ellos, resulta destacable la falta de integración de ciertos datos con potencial discriminatorio en la lista taxativa de datos sensibles[16]; la incertidumbre en torno al uso de *proxies* y datos inferidos que funcionalmente actúen como datos sensibles[17]; los recurrentes problemas prácticos en torno a la correcta aplicación de excepciones a la prohibición del tratamiento de datos sensibles[18]; la falta de transparencia de ciertos sistemas de

---

[11] Artículo 3. r) DSA.

[12] Art. 4.4) RGPD. El RGPD pone como ejemplo de evaluación de aspectos personales actividades tales como 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.

[13] Para una clasificación de la publicidad online, vid. Sartor (2021).

[14] Cfr. Considerando 69 DSA.

[15] Vid. Art. 9.1. RGPD. Bajo la categoría de datos sensibles —denominados categorías especiales de datos— el RGPD se refiere exclusivamente a 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».

[16] Malgieri (2018), págs. 14-16.

[17] Wachter (2019), págs. 436-449.

[18] Tzanou 2020), págs. 449-70.

IA[19]; o la falta de inclusión de algunas excepciones en el RGPD para fines que sí podrían ser beneficiosos, como la corrección de sesgos en los sistemas de IA[20].

Esta primera laguna se retroalimenta con una segunda, la cual no es otra que el ámbito personal de la prohibición: las plataformas en línea a las que se dirige la DSA. Dado que la actividad prohibida es «presentar» el tipo de publicidad descrita, con la normativa vigente no se impide de forma absoluta que las plataformas traten una cantidad inconmensurable de datos sensibles y transmitan dichos datos a servicios de terceros, siempre que se cumpla con alguna de las excepciones legales aplicables, como puede ser el consentimiento del sujeto de datos. Si estos otros servicios no caen bajo la definición de plataformas en línea de la DSA, los mismos podrían presentar publicidad basada en perfiles utilizando datos sensibles, puesto que durante el proceso de redacción de la norma se interpretó que la principal amenaza a efectos de técnicas comerciales manipulativas se planteaba en las plataformas en línea[21].

Surge la duda, en este punto, de si los prestadores de plataformas en línea podrían compartir datos sensibles con otros servicios del mismo grupo, especialmente con aquellos que no estén sujetos a la prohibición al no ser calificados como servicios de plataforma. Responderemos a continuación a dicha cuestión.

III. EL REGLAMENTO DE MERCADOS DIGITALES COMO SOLUCIÓN PROBLEMÁTICA A CIERTAS CARENCIAS DEL ÁMBITO MATERIAL DE LA PROHIBICIÓN

Actualmente, los proveedores de servicios de plataforma cubiertas por la DSA, particularmente aquellas denominadas de muy gran tamaño, pueden quedar asimismo sujetos a las previsiones del Reglamento de Mercados Digitales[22] si cumplen con los requisitos para ser calificados como «guardianes de acceso»[23]. Este es el caso de Meta, empresa designada por la Comisión Europea como guardián de acceso, y al mismo tiempo proveedora de servicios de plataforma en el sentido de la DSA como Facebook e Instagram[24]. La cuestión que aquí exponemos es si la DMA aporta alguna vía para impedir que los guardianes de acceso que presten servicios de plataforma compartan datos sensibles con servicios de terceros o del mismo grupo que no sean calificados como servicios de plataforma y que, en consecuencia, no estén sujetos a la prohibición de emitir publicidad basada en perfiles usando datos sensibles. Siguiendo el ejemplo de Meta, planteamos si hay alguna prohibición que le impida compartir los datos sensibles que obtenga a través de Facebook con otros servicios que preste, como Instagram, o con servicios de terceros.

---

[19] Caplan (2018) version online; Krupiy (2021) versión online.

[20] Bekkum van (2023) versión online.

[21] Laux (2021), págs. 1-11.

[22] 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 (DOUE-L-2022-81470). En adelante, por sus siglas en inglés, «DMA».

[23] Vid. arts. 2 (1) y (3) DMA.

[24] EUROPEAN COMMISSION PRESS CORNER, «Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engine»; EUROPEAN COMMISSION PRESS CORNER, «Digital Markets Act: Commission designates six gatekeepers».

La primera prohibición de la DMA que, en una primera lectura, puede estar más relacionada con la publicidad basada en perfiles es aquella que prohíbe el tratamiento, con el fin de prestar servicios de publicidad en línea, de datos personales de los usuarios finales que utilicen servicios de terceros que hagan uso de servicios básicos de plataforma del guardián de acceso[25]. La clara intención del legislador comunitario con esta prohibición es evitar que los guardianes de acceso adquieran una desmedida ventaja competitiva al tratar datos de usuarios finales de terceros que usen sus servicios de plataforma, si bien también se protege, de forma indirecta, a los usuarios finales[26]. Esta prohibición, sin embargo, no impide la transferencia en la dirección opuesta, es decir, que sea el guardián de acceso el que transfiera los datos personales de sus propios servicios de plataforma a servicios de terceros.

Ahora bien, la DMA establece otras dos prohibiciones que sí pueden resultar de utilidad para complementar la prohibición de la DSA en un extremo: evitar la transferencia de datos personales entre servicios del mismo guardián de acceso. Estas prohibiciones son i) 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, y ii) 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[27]. Bajo ambas, lo que se pretende evitar es que los guardianes de acceso tengan una especial ventaja competitiva al combinar datos personales del servicio básico de plataforma con otros servicios del guardián de acceso o de terceros[28]. De forma transversal, también se incrementa la protección de los usuarios finales en términos de privacidad, lo cual es un claro reflejo de la creciente tendencia comunitaria de aunar los objetivos entre el binomio competencia-protección de datos[29].

Sin embargo, las anteriores prohibiciones quedan limitadas en gran medida por la remisión final que realiza la DMA a la normativa de protección de datos. Así, señala la DMA que las mismas se aplican salvo que se le haya presentado al usuario final «esa opción específica y este haya dado su consentimiento» en el sentido del RGPD, y sin perjuicio de que el guardián de acceso base el tratamiento en las excepciones de i) necesidad para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; ii) necesidad para proteger intereses vitales del interesado o de otra persona física; o iii) necesidad para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento[30]. Una vez más, el Paquete de Servicios

---

[25] Vid. art. 5.2.a) DMA. Lo que prohíbe la DMA bajo esta previsión es, por ejemplo, que Meta utilice los datos personales de otras empresas que incorporan el sistema de «Me gusta» o de inicio de sesión de Facebook en sus plataformas en línea.

[26] Cauffman (2021), págs. 1-10.

[27] Art. 5.2. b) y c) DMA.

[28] Fafchamps (2021), págs. 1-10.

[29] 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). En dicha sentencia, el Tribunal aclaró no sólo la necesidad, sino la obligación de cooperación entre las autoridades nacionales de competencia y protección de datos. En este mismo sentido ya se venían pronunciando previamente otros autores. Vid. Koolen (2023), págs. 427-467.

[30] Art. 5.2 DMA

Digitales hereda las carencias del RGPD, lo cual se evidencia especialmente en la inclusión del consentimiento del sujeto de datos como excepción a las anteriores prohibiciones. Prueba de esta inseguridad es que, a finales de marzo de 2024, la Comisión Europea haya abierto investigaciones por infracción de las anteriores prohibiciones de la DMA contra el modelo *pay-or-okay* (también denominado *pay-or-consent*) implementado por Meta. Conforme al comunicado oficial de prensa, «a la Comisión le preocupa que la elección binaria impuesta por el modelo de »pago o consentimiento» de Meta no ofrezca una alternativa real en caso de que los usuarios no den su consentimiento, con lo que no se logrará el objetivo de evitar la acumulación de datos personales por parte de los guardianes de acceso"[31].

Tanto en la DMA como en la DSA, resulta evidente que el foco se ha puesto en los servicios de plataforma, tanto por la especial influencia que tienen en la vida diaria de los usuarios como por los particulares riesgos que presenta el control de datos para la libre competencia[32]. Sin embargo, el modelo *pay-or-okay* no ha sido implementado sólo por Meta, sino que también ha sido adoptado por otros servicios en línea que, al no ser servicios de plataforma, no están sujetos a las anteriores prohibiciones, así como tampoco a la prohibición de emitir publicidad basada en perfiles usando datos sensibles. Si la Comisión y el Comité Europeo de Protección de Datos basan sus próximas decisiones sobre la legalidad del consentimiento *pay-or-okay* en el RGPD exclusivamente, tales decisiones podrán afectar indirectamente no sólo a los servicios de plataforma, sino también a otros servicios, ya que el RGPD no distingue entre industrias en lo referente a la validez del consentimiento. Por razones de actualidad, hemos decidido abordar en las próximas paginas ciertos servicios que tratan cantidades considerables de datos sensibles, que no son calificados como servicios de plataforma y que se están uniendo al modelo *pay-or-okay*[33]. Bajo el término *«pay-or-okay»* nos referiremos en las próximas páginas a aquel modelo contractual mediante el cual el proveedor otorga al destinatario del servicio dos opciones: o bien pagar una cuota, o bien aceptar la recepción de publicidad y el tratamiento de datos personales con diversos fines.

IV. CRÍTICA AL ÁMBITO PERSONAL DE LA PROHIBICIÓN. A PROPÓSITO DEL AUGE DEL MODELO PAY-OR-OKAY

1. El ámbito personal de la prohibición. Servicios relevantes excluidos

En los últimos años, se ha puesto de manifiesto que muchos operadores digitales han comenzado a usar datos sensibles de usuarios con fines publicitarios que, a menudo, resultan en efectos gravemente adversos para los destinatarios[34]. Aunque muchos de estos servicios, como las redes sociales, están sujetos

[31] EUROPEAN COMMISSION PRESS CORNER, «Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act».

[32] Di Porto (2021), págs. 17-29.

[33] En tanto que ni la Comisión (en materia de competencia) ni el CEPD (en materia de protección de datos) se han pronunciado directamente con respecto a la legalidad del modelo *pay-or-okay* integrado por Meta a fecha de depósito del presente trabajo (30 de marzo de 2024).

[34] Ya en 2016, ProPublica publicó una serie de informes que revelaban que Facebook permitía a los anunciantes excluir a ciertos grupos de anuncios sobre alojamiento, empleo o contratos de crédito basándose en la etnia. Vid. Parris (2016) versión online. Este tipo de discriminación publicitaria es posible gracias al acceso a una gran cantidad de datos sensibles, no sólo derivados de las propias declaraciones del usuario, sino también por las interacciones y reacciones de este en el servicio. A título de ejemplo, hay estudios que muestran como los *likes* de Facebook pueden utilizarse para predecir de forma automática y precisa características sensibles como

a la DSA, no recae sobre ellos ninguna prohibición absoluta en lo relativo al tratamiento y la transferencia de datos sensibles a otros servicios, que pueden no estar sujetos a la prohibición al no caer bajo la definición de «servicios de plataforma»[35]. Este ámbito personal implica la exclusión de ciertos servicios que son relevantes tanto por su número de usuarios como por la cantidad de datos sensibles que manejan, así como por la implementación de modelos *pay-or-okay* que ponen en entredicho la libertad de consentimiento de los destinatarios. Entre otros, podemos citar los servicios de vídeo a la carta por suscripción, como Netflix, Amazon Prime, Disney+ o HBO, así los como servicios de noticias online[36]. La cuestión de política normativa *de lege ferenda* que aquí se plantea es si es necesario que esta prohibición alcance también a este tipo de servicios, especialmente a aquellos que se basan en el modelo *pay-or-okay*, o si es suficiente con que mantengamos la vía *de lega lata,* resultando de aplicación la normativa general de protección de datos.

Comenzando por el ejemplo de los servicios de vídeo a la carta por suscripción, es reseñable que los mismos ya tienen acceso a una vasta cantidad de datos sensibles a través de su propio servicio, con independencia de si servicios de plataforma como Facebook le transfieren o no sus datos. La misma Netflix reconoce analizar sus datos mediante sistemas de *deep learning* para recomendar contenido[37], siendo su sistema alimentado con *inputs* como los datos de búsqueda de usuarios, la clasificación del contenido de menos favorito a más favorito, encuestas para elegir «el mejor» de dos elementos, o el seguimiento del historial de visualización de los usuarios[38]. Los anuncios de Netflix también han comenzado a seleccionarse conforme a sistemas de *deep learning*, especialmente desde que dicho servicio comenzase a ofrecer un modelo más económico, bajo el cual, por una tarifa mensual inferior, el usuario acepta la recepción de anuncios durante la visualización del contenido[39]. La cantidad de inferencias masivas de datos sensibles que puede realizar Netflix, con 260 millones de suscriptores mundiales nada más que en el último cuatrimestre de 2023[40], nos hace plan-

---

«la orientación sexual, la etnia, las opiniones religiosas y políticas, los rasgos de personalidad, la inteligencia, la felicidad, el consumo de sustancias adictivas, la separación de los padres, la edad y el sexo». Uno de estos estudios se basó en un conjunto de datos de más de 58.000 voluntarios, que proporcionaron tanto sus *likes* de Facebook como sus perfiles demográficos detallados y los resultados de varias pruebas psicométricas. El modelo discriminó correctamente entre hombres homosexuales y heterosexuales en el 88% de los casos, entre afroamericanos y caucásicos en el 95% de los casos, y entre demócratas y republicanos en el 85% de los casos. Vid. Kosinski (2013) págs. 5802-5805. Tampoco debemos pasar por alto que el mero acceso a algunos servicios —como a determinadas aplicaciones de citas o a páginas webs con contenido sexual— es ya un indicador de datos sensibles tales como la orientación sexual o la vida sexual del individuo. Vid. Georgieva (2020), págs. 365-384.

[35] La DSA define una plataforma en línea como un servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad de la DSA.

[36] Michinelli (2023), págs. 45-60.

[37] Steck, (2021), págs.7-18.

[38] Steck, (2021), págs.7-18.

[39] Aunque no sea el objeto de este trabajo, en este punto, podría plantearse si la publicidad personalizada en Netflix se acota solo a los anuncios que el usuario recibe a modo de «intermedio publicitario» durante la visualización del contenido, o si las propias recomendaciones también obedecen a un propósito publicitario, en caso de que el orden de estas no obedezca exclusivamente a los intereses del usuario, sino también a las remuneraciones prestadas por los anunciantes.

[40] Statista, «Number of Netflix paid subscribers worldwide from 1st quarter 2013 to 4th quarter 2023», disponible en *https://www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subs-*

tearnos si resulta necesario que la prohibición se aplique también a los grandes servicios de vídeo a la carta por suscripción.

Un fenómeno similar ha comenzado a surgir con los periódicos digitales, conocidos por ser uno de los principales servicios online que basan su modelo de negocio en la publicidad. Con el auge del *Big Data*, el valor económico de los datos ha cobrado una importancia vital[41]. Con esta nueva prioridad en escena, muchos servicios han centrado su atención en la monetización de los datos personales de sus usuarios, comenzando por los periódicos en línea, precursores del modelo *pay-or-okay.* Si bien los modelos de pago llevan años implementándose, bajo este nuevo modelo, la alternativa de pago ya no tiene como núcleo principal o exclusivo que el usuario no se vea expuesto a anuncios, sino que el protagonismo radica en que el usuario no sea objeto de un tratamiento automatizado de datos personales con fines publicitarios. La diferencia puede parecer sutil, pero no es en absoluto baladí. Si bien la recepción de publicidad puede constituir una clara inferencia en la esfera privada de los individuos, el tratamiento de datos personales con fines de elaboración de perfiles publicitarios va un paso más allá, ya que permite al anunciante acudir a sistemas muchos más intrusivos, a menudo nublando la diferencia entre la persuasión y la manipulación algorítmica[42].

Anteriormente, planteábamos la cuestión *de lege ferenda* de si la prohibición de la DSA debe extenderse a los servicios que no son de plataforma, o si es suficiente con que se les aplique la normativa de protección de datos. En este extremo, el modelo *pay-or-okay* es un ejemplo perfecto para evidenciar la inseguridad jurídica que rodea la aplicación del RGPD. Si el modelo *pay-or-okay* es aceptado, esto significará que cualquier servicio, ya sea o no de plataforma, podrá poner un precio a la opción de «rechazar» tratamientos no necesarios de datos personales, ya sean sensibles o no sensibles. Por el especial impacto que este modelo puede tener en el mercado y en la privacidad de millones de usuarios, pasaremos a continuación a analizar los principales argumentos a favor y en contra de la legalidad del *pay-or-okay.*

2. El modelo pay-or-okay. Análisis de su legalidad y cuestiones a resolver

Pese a que el modelo *pay-or-okay* se formulase en sus orígenes como una vía para proteger a los periódicos digitales frente a las *Big Tech*, contando inicialmente con la aprobación condicionada de varias autoridades de protección de datos como la alemana[43], la francesa[44] y la española[45], se ha convertido en

cribers-worldwide/#:~:text=Netflix%20had%20around%20260%20million,compared%20with%20the%20previous%20quarter.

[41] Durovic (2021), págs. 701-710

[42] Hacker (2021), págs. 1-34.

[43] 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», disponible en *https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf*

[44] 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 disponible en https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation

[45] 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

un arma de doble filo, al estar siendo también utilizado por las propias *Big Tech*[46/47]. En la actualidad, Meta escuda la legalidad de su modelo *pay-or-okay* en una resolución del TJUE, emitida a raíz del caso *Meta Platforms Inc. v. Bundeskartellamt* [48]. Aunque la cuestión prejudicial no era directamente relativa a la legalidad de este modelo, 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 «a cambio de una remuneración adecuada, una alternativa equivalente no acompañada de tales operaciones de tratamiento de datos»[49].

Las reacciones al modelo *pay-or-okay* de Meta han sido considerables. En enero de 2024, las autoridades de protección de datos de Holanda, Alemania y Noruega solicitaron al CEPD que se pronunciase sobre la legalidad del *pay-or-okay*[50]. A principios de marzo de este mismo año, 28 ONGs enviaron también una carta abierta al CEPD para que se pronunciase sobre este mismo extremo[51]. Poco después, 39 miembros del Parlamento Europeo han solicitado abiertamente a Meta que deje de usar este modelo, sosteniendo que «la privacidad no puede convertirse en un lujo»[52], y la Comisión Europea ha abierto investigaciones contra Meta por posible infracción de la DMA mediante el modelo *pay-or-okay*[53]. Los principales argumentos que pueden esgrimirse en contra del modelo de consentimiento del *pay-or-okay* pueden sintetizarse, a nuestro entender, en tres aspectos.

El primer aspecto controvertido es el carácter «libre y genuino» del consentimiento de los sujetos de datos. El RGPD exige que el consentimiento al tratamiento de datos debe ser libre[54], sin embargo, multiplicidad de voces conocidas en el ámbito de la privacidad, como la de Max Schrems, han puesto en

---

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.

[46] España tampoco ha sido ajena a la vulnerabilidad de los periódicos frente a las plataformas. Un ejemplo fue que, a finales de 2023, diversos periódicos españoles demandaran a Meta por competencia desleal, alegando el incumplimiento de la normativa de protección de datos para atraer publicidad. Vid. *https://elpais.com/economia/2023-12-04/los-periodicos-espanoles-demandan-a-meta-por-competencia-desleal-y-le-exigen-550-millones.html*

[47] En el caso de Meta, entendemos que implantó dicho modelo como consecuencia de diversas decisiones vinculantes del Comité Europeo de Protección de Datos (en adelante, «CEPD») que declaraban ilícita la base legal utilizada por Meta para procesar datos personales con fines de publicidad comportamental. Vid. 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).*

[48] 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).

[49] Párrafo 150 de la sentencia.

[50] Comunicado emitido en la web oficial de la Autoridad Holandesa de Protección de Datos («Autoriteit Persoons Gegevens»), disponible en *https://autoriteitpersoonsgegevens.nl/actueel/ap-privacy-is-een-grondrecht-niet-alleen-voor-rijke-mensen*

[51] NOYB, «28 NGOs Urge EU DPAS To Reject »Pay Or Okay" On Meta", disponible en *https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta*

[52] MEPs, «Letter-to-Meta-on-Pay-or-Okay», disponible en *https://www.patrick-breyer.de/wp-content/uploads/2024/03/MEPs-Letter-to-Meta-on-Pay-or-Okay.pdf*

[53] EUROPEAN COMMISSION PRESS CORNER, «Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act».

[54] Art. 4.11) RGPD

entredicho que el consentimiento sea libre cuando la única alternativa sea pagar una suma considerable, convirtiendo el derecho a la privacidad en un privilegio para aquellos que puedan permitírselo económicamente[55]. Haciendo una sencilla comparación, puede resultar extraño que actividades como premarcar una casilla para la aceptación del tratamiento, o mover la opción de rechazar a una segunda capa, hayan sido declaradas ilícitas por el TJUE en el caso *Planet49 56*, y, en cambio, el modelo *pay-or-okay* se haya visto aceptado en cierta medida en el caso *Meta Platforms Inc. v. Bundeskartellamt.* Con aquellas, el diseño es el único elemento que dificulta acceder a la opción de rechazar el tratamiento, mientras que, con el *pay-or-okay,* se pone directamente un precio a la opción de rechazar. Desde nuestra perspectiva, esta última práctica es mucho más intrusiva que las anteriores, ya que afecta no a la forma, sino al propio contenido de las condiciones del servicio.

El segundo elemento criticable gira en torno a la granularidad del consentimiento. Según el RGPD, el consentimiento debe ser específico[57], y las directrices del CEPD aclaran que el consentimiento debe poder prestarse de forma separada cuando los fines son diversos entre sí[58]. Sin embargo, en la opción «gratuita» de servicios como Facebook el usuario consiente en un mismo paquete el tratamiento de datos personales con una amalgama de fines, como fines de seguimiento, fines de publicidad personalizada, fines de personalización de funciones, contenido y recomendaciones, o fines de medición y análisis por terceros[59]. Un fenómeno similar ocurre con los periódicos en línea. Cuando el modelo se implementó por primera vez por el periódico austríaco *Der Standard,* algunas instituciones ya comenzaron a advertir que exigir un mismo consentimiento para diversos fines de tratamiento —en este caso, con fines publicitarios, fines de personalización y transferencia a terceros— iba en contra de la normativa de protección de datos[60]. Dicha falta de granularidad se ha extendido también a los modelos implementados por los periódicos digitales españoles[61].

El tercer aspecto controvertido es el concepto de una remuneración «adecuada». Conforme a la STJUE *Meta Platforms Inc. v. Bundeskartellamt,* el proveedor de la red social puede ofrecer una alternativa a operaciones particulares de tratamiento de datos que no sean necesarias (como la publicidad comportamental) a cambio de una remuneración adecuada. En este sentido, la adecuación

---

[55] NOYB, "«Pay Or Okay» - The Beginning Of The End?", disponible en *https://noyb.eu/en/pay-or-okay-beginning-end*

[56] Sentencia del Tribunal De Justicia (Gran Sala) de 1 de octubre de 2019, asunto C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV y Planet49 GmbH, (ECLI:EU:C:2019:801)

[57] Art. 4.11) RGPD

[58] Por todas, vid. CEPD, «Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679», 2020.

[59] Vid. Política de privacidad de Facebook, disponible en *https://www.facebook.com/privacy/policy?section_id=2-HowDoWeUse*

[60] NOYB, "«Pay Or Okay» Bei Derstandard.At", disponible en *https://noyb.eu/en/pay-or-okay-bei-derstandardat*

[61] Poniendo como ejemplo a *El País*, en caso de que el usuario opte por la opción titulada «Navegación gratuita mediante la aceptación de cookies», el mismo aceptará en un mismo paquete las siguientes actividades y fines: almacenamiento y acceso a la información; compartir datos y perfiles para análisis y publicidad personalizada de los anunciantes para nuestras campañas publicitarias; compartir datos y perfiles para análisis y publicidad personalizada de los anunciantes y agencias publicitarias en internet; datos de localización geográfica precisa e identificación mediante análisis de dispositivos; publicidad y contenido personalizados, medición de publicidad y contenido; e investigación de audiencia y desarrollo de servicios.

juega como una suerte de concepto jurídico indeterminado. Entre las dudas que suscita su empleo, nos planteamos si el efecto dominó que puede jugar la aceptación el modelo *pay-or-okay* será un factor para considerar la adecuación de la remuneración[62].

A nuestro entender, el hecho de que un servicio como Facebook exija una remuneración a cambio de no tratar datos personales con fines más allá de los estrictamente necesarios no es causa, *per se*, de ilicitud conforme a la normativa de protección de datos. Así parece que lo entendió también el TJUE en el caso *Meta Platforms Inc. v. Bundeskartellamt*[63]*,* si bien se ha señalado en ciertos sectores que la referencia a la remuneración adecuada en dicha sentencia fue un *obiter dictum,* es decir, una consideración adicional del tribunal no directamente relacionada con la cuestión prejudicial, y, por tanto, no vinculante[64], postura con la que nos encontramos en desacuerdo. Es comprensible, bajo el derecho a la libertad de empresa, que Meta intente optar por bases legales que sean rentables para su modelo de negocio. Cuestión bien distinta es si este modelo se basa en una remuneración desproporcionada que ponga en entredicho la libertad de consentimiento del sujeto de datos. Prevemos que esta adecuación es un tema que aclarará el CEPD a través de una decisión vinculante, y que probablemente trate el TJUE a raíz de futuras cuestiones prejudiciales. En todo caso, se plantea como una cuestión de imperiosa seguridad jurídica que se establezcan unos criterios claros y objetivos que deriven en el denominado efecto Bruselas [65], evitando posibles pronunciamientos contradictorios por las autoridades nacionales de protección de datos.

Pasando a posibles soluciones, consideramos que existen algunos mecanismos para que el modelo *pay-or-okay* sea regulado de una forma proporcional. El primero sería analizar si el responsable de datos goza de una posición dominante, para lo cual sería necesaria la colaboración de las autoridades de competencia. Siguiendo el controvertido caso *Meta Platforms Inc. v. Bundeskartellamt,* el TJUE ya declaró que la posición dominante no es un factor determinante, pero sí relevante, para determinar si el consentimiento ha sido prestado de forma libre. Apreciar la concurrencia de una posición dominante podría moderar el hecho de que el RGPD no establezca distinciones entre industrias en lo relativo a los requisitos aplicables a la legalidad del consentimiento, que es donde radica la principal problemática del modelo *pay-or-okay*. Prevemos, en este sentido, que futuras decisiones de la Comisión Europea contra el modelo *pay-or-okay* de Meta girarán en gran medida en torno a este factor.

---

[62] En sentido afirmativo responden ciertas instituciones, al señalar que, a los diez meses de que la autoridad alemana de protección de datos aceptase el modelo de pago iniciado por los periódicos digitales, al menos 500 páginas webs implementaron este modelo. Considerando que la media de aplicaciones instaladas en un smartphone asciende a 35, se calcula que cada usuario tendría que hacer frente a un gasto de alrededor 8.815,80 euros anuales si las mismas optan por un precio igual al de Meta. En el caso de las páginas webs, en España, el coste promedio de acceder a la versión de pago por acceder a las 100 páginas webs más visitadas del país ascendería a 1.463 euros. Vid. NOYB, "«Pay Or Okay»: 1,500 € A Year For Your Online Privacy?" disponible en *https://noyb.eu/sites/default/files/styles/media_xlarge/public/2024-03/pay_or_okay_map_price_tags_2.2.png?itok=UyiCIqXQ* y GOOGLE/IPSOS, U.S., «How People Discover, Use, and Stay Engaged With Apps, based on smartphone users aged 16-64», disponible en *https://www.thinkwithgoogle.com/marketing-strategies/app-and-mobile/average-number-of-apps-on-smartphones/*

[63] Párrafo 150 de la STJUE *Meta Platforms Inc. v. Bundeskartellamt*

[64] NOYB, «Meta (Facebook / Instagram) To Move To A »Pay For Your Rights" Approach", disponible en *https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach*

[65] Bradford (2020), version online.

El segundo mecanismo sería establecer una tercera opción que sea menos intrusiva, como puede ser aceptar la recepción de publicidad que no esté basada en la elaboración de perfiles, lo cual también contribuiría a que el consentimiento se preste de una forma más libre y granular. Sin embargo, por parte de los prestadores del servicio, podría argumentarse que esta tercera opción solo les resulta viable si continúan recibiendo una remuneración a cambio, ya que este otro modelo publicitario resulta considerablemente menos efectivo. Es reseñable, en este sentido, que la DSA ha introducido una nueva obligación para 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, al exigir que ofrezca al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles[66]. Esta obligación sólo se estableció para los sistemas de recomendación, por lo que, en principio, no se dirige hacia la publicidad que no esté inserta en los mismos. La DMA, en el caso de los guardianes de acceso, también recomienda la inserción de una alternativa equivalente pero menos personalizada en los servicios de plataforma, si bien esta fórmula sólo se llegó a incluir en los considerandos de la norma[67]. Aun así, se está apreciando una creciente tendencia comunitaria a fomentar la inserción de una opción menos personalizada no basada en perfiles, como puede desprenderse, por ejemplo, del borrador del compromiso de *cookies* publicado por la Comisión Europea recientemente[68].

En conclusión, cabe destacar que la regulación del tratamiento de datos sensibles y no sensibles con fines de publicidad basada en perfiles todavía deja muchos interrogantes, como encontrar un justo balance entre los intereses económicos de los servicios digitales y la inserción de bases legales que respeten la libertad de consentimiento. Por las razones anteriormente expuestas, nos atrevemos a predecir que es poco probable que el CEPD declare la ilicitud de todo modelo de tratamiento basado en el sistema *pay-or-okay*, si bien resta aclarar ciertas controversias, como qué se entiende por una remuneración adecuada, o el desarrollo de directrices para integrar la posición de dominio en el examen de licitud del consentimiento.

V. CONSIDERACIONES FINALES

Durante el presente trabajo, se han analizado críticamente los principales déficits de la prohibición de presentar publicidad basada en perfiles usando datos sensibles, y se han propuesto ciertas medidas para paliarlos. A nuestro entender, el legislador comunitario perdió la oportunidad de ofrecer una protección reforzada con respecto a ciertas prácticas comerciales que pueden resultar manipulativas al basarse en datos que revelan posibles vulnerabilidades de los destinatarios, como es el caso de los datos reveladores de la situación económica del individuo. Igualmente, la propia actividad prohibida, «presentar» publicidad basada en perfiles usando datos sensibles, deja de lado la raíz de la problemática, que es el tratamiento de dichos datos.

---

[66] Art. 38 DSA

[67] Vid. Considerando (36) DMA

[68] EUROPEAN COMMISSION, «Cookie pledge», available at *https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en*

La principal carencia que hemos detectado en la prohibición es su excesiva dependencia o confianza en el RGPD, pese a las evidentes limitaciones que el mismo presenta en la práctica. Estas limitaciones se plasman de una manera evidente en el actual debate sobre la legalidad del modelo *pay-or-okay*, en el cual se están basando tanto aquellos servicios cubiertos por la norma, como las redes sociales, como otros no cubiertos, siendo el caso de los periódicos en línea y las plataformas de vídeo a la carta por suscripción. Entendemos que la viabilidad del modelo de negocio de estos servicios exige una remuneración a cambio, ya sea a través de una remuneración directa por parte de los usuarios, ya sea a través de la publicidad.

Sin embargo, bajo el modelo *pay-or-okay,* se pone un precio a la opción de rechazar el tratamiento de datos personales con fines no necesarios y diversos entre sí, lo cual pone en entredicho la licitud de este consentimiento. La libertad que debe caracterizar el consentimiento es todavía más acotada en el caso de los modelos *pay-or-okay* implementados en grandes plataformas como Facebook, en las que el usuario se ve inmerso en un efecto *lock-in*. Por esta razón, sostenemos que el análisis de la legalidad del *pay-or-okay* no debe restringirse exclusivamente al RGPD, sino que debe tener en cuenta otros factores, como la posición de dominio del prestador del servicio, o si el mismo guarda la condición de guardián de acceso conforme a la DMA. En todo caso, para la solución de estas cuestiones, se plantea como un imperativo la futura colaboración entre las autoridades de protección de datos y de competencia.

VI. BIBLIOGRAFÍA

AEDP (2024) «*Guía sobre el uso de cookies*», págs. 29-30.

Bekkum Van, Marvin and Zuiderveen, Frederik (2023), «Using sensitive data to prevent AI discrimination: Does the EU GDPR need a new exception?» *Computer Law and Security Review*, 48 [Online].

Bradford, Anu (2012). «The Brussels Effect», *Northwestern University Law Review*, 107(1), págs. 1-68.

Caplan, Robyn et al. (2018), «Algorithmic Accountability: A Primer. Data & Society report» [Online] Available at: https://datasociety.net/library/algorithmic-accountability-a-primer/

Castillo Parrilla, José Antonio (2023), «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, págs. 53-88.

Cauffman, Caroline and Goanta, Catalina (2021), «A New Order: The Digital Services Act and Consumer Protection», *Cambridge University Press,* págs. 1-10.

Collado-Rodríguez, Noelia (2023), «La evaluación de la solvencia mediante el uso de sistemas de IA. Creditworthiness assessment by AI», *Revista CESCO,* págs. 41–67.

Di Porto, Fabiana et al. (2021,) «A computational analysis of the DMA and DSA», *Computational Antitrust Journal,* págs. 17-29.

Durovic, Mateja and Lech, Franziska (2020), «A consumer Law Perspective on the Commercialization of Data», *European Review of Private Law 5,* págs. 701-710.

Edelson, Laura et al (2023), «Access to data and algorithms: for an effective DMA and DSA implementation», *CERRE,* págs. 46-53.

Fafchamps, Nicolas and Hornkohl, Lena (2021), «Changed Policies of GAFAs, Limited Impact of DMA/DSA on Targeted Ads: Competition Law as the Solution?», *Kluwer Competition Law Blog,* [Online].

GALLI, Federico (2022), «Predictive Personalisation» in GALLI, F. *Algorithmic Marketing and EU Law on Unfair Commercial Practices*, Springer, págs. 81-107.
GEORGIEVA, Ludmila and KUNER, Christopher (2020), «Article 9 Processing of special categories of personal data» in KUNER C. et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary,* Oxford Academic, págs. 365-384.
GONZÁLEZ CABAÑAS, José, CUEVAS, Ángel and CUEVAS, Rubén (2018), «Facebook use of sensitive data for advertising in Europe», *27th USENIX Security Symposium*, págs. 479-495.
GOOGLE/IPSOS, U.S. (2016) «How People Discover, Use, and Stay Engaged With Apps, based on smartphone users aged 16-64» [Online].
HACKER, Philipp (2021), «Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law», *European Law Journal,* págs. 1-34.
KAMIRAN, Faisal. et al (2013), «Techniques for Discrimination-Free Predictive Models», in Custers B. et al. (eds) *Discrimination and Privacy in the Information Society*, Springer [Online].
KOSINSKI, Michal et al (2013). «Private traits and attributes are predictable from digital records of human behavior*», Proceedings of the National Academy of Sciences (PNAS),* págs. 5802-5805.
KRUPIY, Tetyana (2021), «Why the Proposed Artificial Intelligence Regulation Does Not Deliver on the Promise to Protect Individuals from Harm», *European Law Blog* [Online].
LAUX, Johann et al (2021), «Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA», *Computer Law & Security Review*, págs. 1-10.
LEAVY, Susan (2018), «Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning», *2018 IEEE/ACM 1st International Workshop on Gender Equality in Software Engineering (GE)*, págs. 14-16.
MALGIERI, Gianclaudio and QUINN, Paul (2020). «The Difficulty of Defining Sensitive Data. The concept of sensitive data in the EU data Protection framework», *German Law Journal,* págs. 1583-1612.
MEPs, (2024) «Letter-to-Meta-on-Pay-or-Okay» [Online].
MICHINELLI, Andrea (2023), «I servizi intermediari della società dell'informazione» en BOLOGNINI, Luca, et al. *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Lefebre, págs. 45-60.
NOYB (2024) «28 NGOs Urge EU DPAS To Reject «Pay Or Okay» On Meta», [Online].
NOYB, (2024) "«Pay Or Okay»: 1,500 € A Year For Your Online Privacy?" [Online].
NOYB, (2024) «"Pay Or Okay" - The Beginning Of The End?" » [Online].
PARRIS, Terry and ANGWIN, Julia (2016) «Facebook lets advertisers exclude users by race», ProPublica [Online]
SARTOR, Giovanni et al (2021), *Regulating targeted and behavioural advertising in digital services: how to ensure users' informed consent*, European Parliament.
STATISTA, «Number of Netflix paid subscribers worldwide from 1st quarter 2013 to 4th quarter 2023», 2023 [Online].
STECK, Harald et al (2021), «Deep Learning for Recommender Systems: A Netflix Case Study», *AI Magazine 42(3),* págs. 7-18 [Online]
TZANOU, Maria (2020). «The Future of Eu Data Privacy Law: Towards a More Egalitarian Data Privacy», *Journal of International and Comparative Law* 7, págs. 449–70.
TZOULIA, Eleni (2021). «Targeted advertising in the digital era: Modern challenges to consumer privacy and economic freedom. The responses of the EU legal order», in SYNODINU, T. (ed.) *EU internet law in the digital single market*, Springer, págs. 447-477.
WACHTER, Sandra and MITTELSTADT, Brent (2019). «A Right To Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbian Business Law Review,* págs. 436-449.