



Universidad Internacional de La Rioja
Grado en Derecho

El uso de datos personales para la publicidad en redes sociales y las opiniones políticas

Trabajo de fin de grado presentado por: Claudia Prettner

Titulación: Grado en Derecho

Área jurídica: Derechos fundamentales

Directora: María Lidia Suárez Espino

Ciudad: Bruselas

4 de febrero de 2020

Firmado por: Claudia Prettner

Índice

LISTADO DE ABREVIATURAS	2
RESUMEN	3
ABSTRACT	3
I. INTRODUCCIÓN	4
II. PUBLICIDAD EN REDES SOCIALES	7
1. Perfilado ideológico y propaganda electoral	9
III. NORMAS DE PROTECCIÓN DE DATOS APLICABLES	13
1. Consentimiento del interesado	15
2. Ejecución de un contrato con el interesado	17
3. Intereses legítimos perseguidos por el responsable del tratamiento	18
4. Elaboración de perfiles y decisiones individuales automatizadas	21
IV. TRATAMIENTO DE DATOS PERSONALES RELATIVOS A OPINIONES POLÍTICAS Y ENVÍO DE PROPAGANDA ELECTORAL	23
1. Consentimiento explícito del interesado	24
2. Datos que el interesado ha hecho manifiestamente públicos	25
3. Razones de interés público esencial sobre base de una ley	26
3.1. Artículo 58 bis de la Ley Orgánica del Régimen Electoral General	27
3.1.1. Posiciones de la AEPD	28
3.1.2 Sentencia de inconstitucionalidad	29
V. REDES SOCIALES Y POLÍTICAS DE PRIVACIDAD	31
1. Facebook	31
2. Google	33
3. Twitter	34
VI. CONCLUSIONES	37
BIBLIOGRAFÍA	40

LISTADO DE ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

CE: Constitución Española

CEO: Chief Executive Officer

FTC: Federal Trade Commission

GPS: Global Positioning System

IAB: Interactive Advertising Bureau

Ibid.: Ibidem

IP: Internet Protocol

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

LOREG: Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General

p. ej.: por ejemplo

RGPD: 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)

RTB: Real Time Bidding

SMS: short message service

UE: Unión Europea

RESUMEN

En los últimos años no solo operadores comerciales, sino también actores políticos se sirvieron de las redes sociales para orientar publicidad a los votantes en sus campañas electorales e hicieron uso de datos personales de los usuarios para dirigir anuncios altamente personalizados a ellos. Estas prácticas planteaban cuestiones en lo que concierne el cumplimiento con disposiciones legales sobre protección de datos. Este trabajo aclara las normas de protección de datos aplicables y los fundamentos jurídicos disponibles para el tratamiento de datos personales (inclusive datos llamados «sensibles») con fines de orientación de publicidad personalizada al usuario. A tal efecto, se analizan varias fuentes jurídicas a nivel europeo así como a nivel nacional y se ilustra el trabajo con ejemplos prácticos y jurisprudencia reciente.

Palabras clave: protección de datos, redes sociales, publicidad personalizada, microtargeting, elaboración de perfiles

ABSTRACT

In recent years, not only commercial operators, but also political actors took advantage of social networks to target voters in their electoral campaigns and made use of users' personal data to target highly personalised advertisements to them. Such practices raised questions regarding their compliance with data protection provisions. This thesis clarifies the applicable data protection rules and the legal bases available for the processing of personal data (including so-called "sensitive" data) for the purpose of targeting personalised advertising to the user. To this end, several legal sources at European as well as at national level are analysed and the thesis is illustrated with practical examples and recent jurisprudence.

Keywords: data protection, social networks, personalised advertising, microtargeting, profiling

I. INTRODUCCIÓN

Clic, clic, clic, clic. Cuando hayas leído estas palabras, se habrán realizado unos 300.000 *likes*¹ en Facebook, unos 20.000 Tweets² en Twitter y subido unas 30 horas de video³ en YouTube⁴.

El 85% de los internautas de 16-65 años en España utiliza redes sociales, lo que representa más de 25,5 millones de usuarios⁵.

Antropólogos como Alfred Radcliffe-Brown y John Barnes ya estudiaron el fenómeno de las redes sociales – en sentido clásico – en los años 40 y 50 del siglo XX. Según ellos, una red social es una estructura social formada por personas o entidades conectadas y unidas entre sí por algún tipo de relación o interés común. (RADCLIFFE-BROWN 1940 y BARNES 1954).

Efectivamente, una red social en línea – en el sentido que nos ocupa en este trabajo – tiene fines y características parecidos. Aunque se pueden encontrar definiciones diversas de lo que constituye una red social en línea, parece haber una base común en toda ellas: Podemos entender una red social como una plataforma en línea en la cual se permite, mediante la utilización de perfiles, la comunicación y la interacción entre los usuarios y el intercambio de varios tipos de contenido (p. ej. información, imágenes o videos).

¹ CAREY-SIMOS, G. «How Much Data Is Generated Every Minute On Social Media?». *WeRSM*. 18 agosto 2015. Disponible en: <https://wersm.com/how-much-data-is-generated-every-minute-on-social-media/>.

² Ibid.

³ LOKE HALE, J. «More Than 500 Hours Of Content Are Now Being Uploaded To YouTube Every Minute». *Tubefilter*. 7 mayo 2019. Disponible en: <https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute/>.

⁴ Suponiendo que lees cada “Clic” en un segundo, pues cuatro segundos en total.

⁵ *Estudio Anual de Redes Sociales 2019*, IAB Spain, 2019. Consultado el: 4 noviembre 2019, 16:18. Disponible en: https://iabspain.es/wp-content/uploads/estudio-anual-redes-sociales-iab-spain-2019_vreducida.pdf.

Según el *Estudio Anual de Redes Sociales 2019*⁶ de IAB SPAIN, las redes sociales más utilizadas en España son WhatsApp⁷ (88%), seguida de Facebook (87%), YouTube (68%), Instagram⁸ (54%) y Twitter (50%).

El éxito que pueden acumular estas plataformas se debe, en particular, a su accesibilidad, ya que la utilización de las redes sociales suele ser «gratuita». Es necesario entrecomillar el «gratuito», ya que los proveedores de las redes sociales suelen utilizar otros medios para monetizar sus servicios: obtienen acceso a una enorme cantidad de datos sobre sus usuarios, como sus perfiles sociodemográficos, intereses y preferencias, y utilizan estos datos para dirigir publicidad personalizada a los mismos⁹.

Y este modelo de negocio de las redes sociales nos lleva al núcleo de este trabajo: ¿cómo y para qué fines publicitarios se utilizan los datos personales, qué problemática puede surgir del punto de vista de las normas jurídicas sobre protección de datos y qué papel desempeñan los datos sensibles, como los que se refieren a la ideología de una persona? A continuación, se examinarán técnicas utilizadas en campañas electorales, como el microtargeting, y se utilizará como ejemplo paradigmático el caso de Cambridge Analytica. Seguidamente, el trabajo analizará las normas de protección de datos aplicables, en particular el Reglamento general de protección de datos¹⁰, y las bases jurídicas que pueden autorizar el tratamiento de datos personales para la orientación de publicidad personalizada en las redes sociales con un foco particular en las opiniones políticas. Por último, se analizará también el

⁶ Ibid.

⁷ WhatsApp es una empresa de Facebook. Es controvertido si WhatsApp es una red social o simplemente una aplicación de mensajería instantánea.

⁸ Instagram es una empresa de Facebook.

⁹ GFK CONSORTIUM. *Behavioural Study on Advertising and Marketing Practices in Online Social Media*. European Commission, 2018.

¹⁰ 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).

El uso de datos personales para la publicidad en redes sociales y las opiniones políticas artículo 58 bis de la Ley Orgánica del Régimen Electoral General¹¹ y la declaración de inconstitucionalidad de su apartado 1.

¹¹ Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG).

II. PUBLICIDAD EN REDES SOCIALES

Se dedica este capítulo a conocer el funcionamiento y ecosistema de la publicidad en línea, y en particular en las redes sociales. Este trabajo no trata de analizar la licitud del contenido de los anuncios, que está regulado principalmente en la Ley General de Publicidad¹² y en las normas especiales que regulan determinadas actividades publicitarias, así como en la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias¹³ y en la Ley de Competencia Desleal¹⁴. Sin embargo, para comprender el concepto de publicidad nos referimos a la Ley General de Publicidad, que entiende por publicidad en su artículo 2 «*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*».

Como nos interesamos en particular por la publicidad en redes sociales, debemos analizar el concepto de publicidad comportamental (o publicidad basada en intereses). La publicidad comportamental se basa en la observación del comportamiento y la actividad de los individuos a lo largo del tiempo para – a través de la elaboración de perfiles – proporcionarles publicidad que coincida con sus intereses¹⁵. Para poder dirigir publicidad comportamental es necesario recopilar un gran número de datos relativos al usuario. Esta recopilación se realiza mediante varias técnicas y tecnologías de rastreo, como las cookies y flash cookies, balizas web y huellas digitales de dispositivos (*fingerprinting*), junto a la recopilación de datos realizada en las propias redes sociales. Estas tecnologías permiten el seguimiento del

¹² Ley 34/1988, de 11 de noviembre, General de Publicidad.

¹³ 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.

¹⁴ Ley 3/1991, de 10 de enero, de Competencia Desleal.

¹⁵ GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 2/2010 sobre publicidad comportamental en línea*, GT 171, 2010.

usuario en diferentes dispositivos y la recogida de datos, entre otros, sobre sus compras, actividades e interacciones en las redes sociales, ubicación y hábitos de navegación. De hecho, cuando visitamos un único sitio web, nuestro comportamiento de navegación es por lo general transmitido a más de 100 partes terceras¹⁶.

El mercado de la publicidad en línea es enorme. Según el informe *WARC Global Ad Trends*, publicado en marzo de 2019¹⁷, Facebook y Google recibieron 144.600 millones de dólares (24,5%) de los 590.400 millones destinados a la publicidad en general en todo el mundo en el año 2018. En el segmento de la publicidad en línea, el porcentaje de dinero que fue al duopolio aumenta todavía más y alcanza el 56,4% del gasto publicitario. Efectivamente, la primera fuente de ingresos de las redes sociales proviene de la publicidad.

Los anuncios publicitarios llegan al usuario mediante un sistema automatizado de compra de espacios publicitarios, basado en algoritmos («la compra programática»). Son los algoritmos los que definen los términos de la demanda y ejecutan la compra más adecuada a los objetivos de la campaña – en cuanto a perfiles, precio, valor u otros parámetros identificados por el comprador de los anuncios. (IABpedia, IAB SPAIN¹⁸)

El modelo más común en la compra programática es el *Real Time Bidding* (RTB), que permite adquirir espacios publicitarios en una subasta en tiempo real. En este modelo suelen intervenir un gran número de agentes para cada transacción (por ejemplo, anunciantes, agencias, ad exchanges, DSP [Demand Side Platform], trading desks, redes publicitarias, medios). Las partes esenciales son: i) la demanda, es decir

¹⁶ SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. *EDPS Opinion on online manipulation and personal data*. Opinion 3/2018, 2018.

¹⁷ «Online ad money pool gets shallower for those outside the duopoly». *WARC*. 21 de marzo de 2019. Disponible en: https://www.warc.com/newsandopinion/news/online_ad_money_pool_gets_shallower_for_those_outside_the_duopoly/41839.

¹⁸ «IABpedia. El glosario de términos digitales». *IAB Spain*. Consultado el: 4 noviembre 2019, 16:05. Disponible en: <https://iabspain.es/iab-spain/iabpedia/>.

los anunciantes que están interesados en la difusión de la publicidad en los medios; y ii) la oferta, es decir los medios que buscan ingresos mediante la venta de espacios publicitarios. Entre la oferta y la demanda se sitúa el ecosistema de la compra programática con la bolsa, llamada *Ad Exchange*, en el centro. La *Ad Exchange* es la plataforma donde se realiza la subasta y se producen las transacciones de compra y venta de la publicidad. Las impresiones son adjudicadas a un anunciante tras analizar todas las ofertas registradas por esa misma impresión. Puesto que el anunciante determina qué tipo de perfiles quiere alcanzar en función de una serie de parámetros definidos por él, como por ejemplo edad, sexo, localización e intereses, el valor otorgado a la impresión depende del reconocimiento del perfil del usuario por parte del anunciante. Las subastas duran solo 200 milisegundos, durante el tiempo que la página web se está cargando. Seguidamente, el anuncio ganador aparece instantáneamente en la página que se está visitando.

Google con su amplia red publicitaria (sus anuncios pueden aparecer en lugares como la búsqueda, YouTube y en miles de sitios web asociados) es el modelo paradigmático del sistema de RTB. Facebook utiliza su propio sistema de subasta de anuncios, en el que compiten todos aquellos dirigidos a una audiencia objetivo. Se determina el anuncio ganador basado en tres factores principales: la puja, el porcentaje de acciones (interactuaciones con el anuncio) estimadas y la calidad del anuncio¹⁹. Un procedimiento parecido existe para Twitter, del que cabe mencionar que está asociado a la red publicitaria de Google y usa sus sistemas para comprar y publicar anuncios en Twitter²⁰.

1. Perfilado ideológico y propaganda electoral

El seguimiento constante de las personas en línea a través de varias plataformas (búsquedas, clics en enlaces, interacciones en redes sociales, el tiempo

¹⁹ «Entrega de anuncios». *Facebook*. Consultado el: 4 noviembre 2019, 16:02. Disponible en: <https://es-es.facebook.com/business/help/430291176997542?id=561906377587030>.

²⁰ «Pujas y subastas». *Twitter*. Consultado el: 4 noviembre 2019, 16:05. Disponible en: <https://business.twitter.com/es/help/troubleshooting/bidding-and-auctions-faqs.html>.

dedicado en cada sitio) hace posible clasificar a las personas según sus atributos y perfiles específicos.

En Facebook, gracias a un análisis basado en la utilización del botón «Me gusta» (*likes*), se podían obtener datos personales sensibles de un usuario como la orientación sexual, etnicidad, opiniones políticas y religiosas, uso de sustancias y otros con una precisión de hasta el 95%²¹ (KOSINSKI, STILLWELL, GRAEPEL 2013). Si estos datos se combinan con otras bases de datos, correos electrónicos, historial de compras y de navegación, dirección IP, puntos de acceso WiFi etc., se pueden inferir incluso atributos personales más profundos y utilizar estos conocimientos para dirigirse al público de manera personalizada.

En 2016, una investigación efectuada por *ProPublica*²² reveló que Facebook usaba más de 52.000 atributos únicos para clasificar a sus usuarios, atributos que podían ser explotados por los compradores de anuncios. De hecho, una gran variedad de actores puede estar interesada en dirigir mensajes personalizadas a un grupo de personas clasificadas según atributos demográficos, psicológicos, políticos u otros criterios como su nivel económico, intereses o hábitos. Por ejemplo, en las campañas electorales de los últimos años alrededor del mundo, se utilizaron anuncios políticos personalizados para alcanzar determinados segmentos de la población. Esta segmentación de la audiencia se conoce por el término *microtargeting*, y se basa en el uso de algoritmos para dirigir mensajes personalizados a un segmento de la población que comparte cualidades similares. En el contexto político, significa adaptar mensajes a un subgrupo o miembros individuales del electorado, gracias al uso de datos y análisis de los mismos, para establecer una relación con los votantes potenciales²³.

²¹ Grados de precisión: Caucásico vs. Afroamericano 95%, Cristiano vs. Musulmán 93%, Demócrata vs. Republicano 85%, Lesbiana 75%, Gay 88%, Fuma cigarrillos 73%, Bebe alcohol 70%, Usa drogas 65%.

²² ANGWIN, J., MATTU S., PARRIS T. «Facebook Doesn't Tell Users Everything It Really Knows About Them». *ProPublica*. 27 diciembre 2016. Disponible en: <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>.

²³ Vease AGAN 2007, BARBU 2013 y BODÓ 2017.

La técnica del *microtargeting* recibió mucha atención pública por el caso de Cambridge Analytica²⁴, en el que datos personales de cuentas de Facebook fueron filtrados a la empresa de dicho nombre para dirigir propaganda electoral altamente personalizada a los votantes. El caso afectó a perfiles de 87 millones de usuarios de Facebook y fue una aplicación llamada *This is Your Digital Life* la que hizo posible la recogida de los datos. La aplicación ofrecía un test de personalidad basado en cinco rasgos de personalidad, conocido como los *Big Five* o OCEAN (Openness to experience; Conscientiousness; Extraversion; Agreeableness; Neuroticism²⁵) y estuvo disponible en Facebook entre 2013 y 2015.

Los usuarios de la aplicación consentían en ceder datos de su cuenta para fines de investigación académica a cambio de una pequeña retribución. Para utilizar la aplicación *This is Your Digital Life*, los usuarios debían prestar su consentimiento para dar acceso a determinados datos de su perfil, como por ejemplo el nombre, datos demográficos, actualizaciones de estado, la utilización del botón «Me gusta» así como a ciertos datos de la lista de sus amigos. Esta última es la razón del gran número de usuarios afectados: aunque el test fue realizado por unos 300.000 usuarios de Facebook, la aplicación tenía también acceso a los datos de sus amigos, sin que ellos pudieran consentir tal acceso, y así la cantidad de perfiles aumentó hasta los 87 millones.

Los resultados de los test de personalidad, junto con otros datos recogidos de la plataforma (p. ej. datos del perfil, *likes* y contenido compartido), fueron filtrados a Cambridge Analytica, que combinó esta información psicológica con otras bases de datos y la cruzó con direcciones, números de teléfonos y correos electrónicos. Así, la empresa utilizó los datos personales de los usuarios de Facebook para diseñar estrategias de campañas electorales altamente personalizadas, basadas en los perfiles psicométricos de los electores.

²⁴ Cambridge Analytica era una empresa privada con sede en Londres (creada en 2013 y disuelta en 2018) especializada en el análisis de datos, con una rama comercial y otra política.

²⁵ Apertura a la experiencia; Conciencia o Responsabilidad; Extraversión; Agradecimiento o Amabilidad; Neuroticismo o Inestabilidad Emocional.

Parece ser que estas técnicas habrían sido utilizadas en varias campañas, siendo los casos más conocidos las elecciones presidenciales estadounidenses de 2016 y el Brexit referéndum de 2016. La campaña electoral de Donald Trump de 2016 invirtió la mayor parte del presupuesto de publicidad digital en Facebook y utilizó diariamente 50.000 anuncios distintos, todos ellos dirigidos a diferentes segmentos del electorado, gracias al análisis efectuado por Cambridge Analytica. La focalización psicométrica de mensajes permite influir en las emociones del votante para persuadirlo de tomar una decisión de voto específica, hasta el punto de poder hablar de manipulación. Queda sin contestar la pregunta de si la victoria de Trump fue – por lo menos parcialmente – debida a su estrategia de propaganda electoral en Facebook basada en la explotación de datos sensibles personales.

A consecuencia del escándalo de Cambridge Analytica, el 24 de julio de 2019, la Comisión Federal de Comercio de Estados Unidos (FTC) anunció una orden de acuerdo con Facebook que impuso el pago de una multa de 5.000 millones de dólares a la empresa por «*engañar a sus usuarios sobre su habilidad de controlar la privacidad de sus datos personales*»²⁶ Como parte del acuerdo – complementario a la multa – Facebook debe implementar una serie de nuevos requisitos de privacidad, modificar su estructura corporativa y crear un nuevo sistema de cumplimiento.

También se han iniciado investigaciones jurídicas en otros países, por ejemplo, en Brasil, Reino Unido y en España. El 5 de abril de 2018, la propia AEPD inició actuaciones de investigación, ya que hasta 137.000 usuarios de Facebook en España podrían haber sido afectados por la transmisión de datos sin su consentimiento a Cambridge Analytica. Las actuaciones de la AEPD se archivaron el 15 de octubre de 2018 por haber prescrito los hechos objeto del análisis. Además, aunque había personas en España que utilizaron la aplicación o tenían amigos que

²⁶ «La FTC impone penalidad de \$5 mil millones y nuevas restricciones de privacidad de gran envergadura a Facebook». *Comisión Federal de Comercio protegiendo a los consumidores*. 24 julio 2019. Disponible en: <https://www.ftc.gov/es/noticias/2019/07/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de>.

utilizaron la aplicación, no se pudo constatar que hubiera habido efectivamente una comunicación de los datos de estos usuarios en España a Cambridge Analytica²⁷.

III. NORMAS DE PROTECCIÓN DE DATOS APLICABLES

En esta sección se analizarán los fundamentos jurídicos de la legislación sobre protección de datos que permiten dirigir publicidad personalizada en redes sociales basada en el tratamiento de datos personales.

El Reglamento (UE) 2016/679, de 27 de abril de 2016, el «Reglamento general de protección de datos»²⁸ (RGPD), entró en vigor el 24 de mayo de 2016 y es aplicable y de obligado cumplimiento en toda la Unión Europea desde el 25 de mayo de 2018. Como Reglamento, es obligatorio en todos sus elementos y directamente aplicable en España, sin que fuera necesario un acto de transposición. El RGPD intenta buscar el equilibrio entre dos fines – proteger los datos personales y garantizar su libre circulación. El RGPD era necesario para adaptar el derecho existente a la evolución tecnológica. Pretende fortalecer los derechos de los individuos, denominados interesados, y darles más control y transparencia sobre el tratamiento de sus datos.

A pesar de ser un Reglamento, el RGPD reconoce en determinados casos, siguiendo el considerando 8, la posibilidad de los Estados miembros para establecer disposiciones nacionales a fin de incorporar elementos del Reglamento a su derecho nacional, así como les concede margen de maniobra para especificar sus normas (véase considerando 10). Por ejemplo, el RGPD concede a los Estados miembros bastante margen de maniobra en su artículo 9 para concretar las bases jurídicas del tratamiento de las categorías especiales de datos personales.

²⁷ Resolución de archivo de actuaciones de la Agencia Española de Protección de Datos. Procedimiento No: E/01873/2018. AEPD, 2018.

²⁸ 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).

A este respecto, el legislador español adoptó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que entró en vigor el 6 de diciembre de 2018. El objetivo de la LOPDGDD es, por un lado, adaptar el ordenamiento jurídico español al RGPD y complementar sus disposiciones y, por otro lado, garantizar los derechos digitales a la ciudadanía.

Este trabajo se focaliza en primer lugar en el RGPD, que proporciona los fundamentos jurídicos principales, para después examinar las particularidades de la LOPDGDD. Analizará en particular el capítulo II del RGPD titulado «Principios», que ofrece las bases jurídicas para dirigir publicidad comportamental mediante el uso de datos personales.

No es objeto de este trabajo la Directiva sobre la privacidad y las comunicaciones electrónicas²⁹ que se aplica al almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario (las cookies), y exige el consentimiento de dicho abonado o usuario para estos fines.

El artículo 5 del RGPD enumera los principios relativos al tratamiento y exige, entre otros, que los datos personales sean tratados de manera lícita, leal y transparente, y que sean recogidos con fines determinados, explícitos y legítimos. No obstante, el precepto que más nos interesa es el artículo 6 del RGPD, que estipula las condiciones de licitud del tratamiento. El RGPD cuenta con seis condiciones, o bases jurídicas legitimadoras, para el tratamiento de datos: i) el consentimiento del interesado para uno o varios fines específicos; ii) la ejecución de un contrato con el interesado; iii) el cumplimiento de una obligación legal del responsable del tratamiento; iv) la protección de intereses vitales; v) el cumplimiento de una misión de interés público; y vi) la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, sujeto a un examen de ponderación.

²⁹ Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). La Directiva está actualmente bajo revisión y la Comisión Europea propuso un Reglamento para derogar la Directiva en 2017 (COM/2017/010 final - 2017/03 (COD)).

Se prescinde del análisis de los números iii, iv y v, ya que se estima que dichas bases jurídicas son menos relevantes para el envío de publicidad a usuarios en redes sociales. Por lo tanto, se procede al análisis en más detalle de los números i, ii y vi, en particular con ayuda de documentos orientadores del Grupo de trabajo sobre protección de datos del artículo 29 (Grupo de trabajo del artículo 29) y del Comité Europeo de Protección de Datos.

1. Consentimiento del interesado

El consentimiento, previsto en artículo 6.1.a RGPD, es la base jurídica legitimadora clave del tratamiento de datos personales. El RGPD contiene en su artículo 4.11 la definición de «consentimiento», entendido como *«toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen»*. El considerando 32 da ejemplos de qué constituye o no constituye consentimiento y clarifica que el silencio, las casillas ya marcadas o la inacción no pueden considerarse consentimiento.

El Grupo de trabajo del artículo 29 elaboró en 2018 unas *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* que clarifican los requisitos necesarios para obtener y demostrar un consentimiento válido. En primer lugar, aclaran que el consentimiento – como manifestación de la voluntad específica – debe obtenerse para todos los fines separadamente, si el tratamiento tiene varios fines. Las Directrices además explican que la «voluntad libre» significa que el interesado debe tener control y capacidad real de elección. Un consentimiento incluido como parte no negociable en las condiciones generales no es considerado prestado libremente. Este punto de vista está reflejado también en el considerando 42 del RGPD que afirma que el consentimiento no se considera prestado libremente *«cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno»*.

El artículo 7.4 RGPD, junto con el considerando 43, contiene directrices adicionales para evaluar si el consentimiento se ha dado libremente. Con esta disposición se pretende evitar vincular el tratamiento de datos personales a la prestación de un contrato o servicio para el cual estos no son necesarios. El artículo

7.4 RGPD exige tener en cuenta esta dependencia para la evaluación de la libre prestación del consentimiento. Siguiendo el considerando 43, no se considera que el consentimiento haya sido prestado libremente en el caso de que se supedita el cumplimiento de un contrato o la prestación de un servicio al consentimiento para el tratamiento de datos personales, cuando dicho tratamiento no es necesario para su cumplimiento. Según el Grupo de trabajo del artículo 29, el consentimiento no debe convertirse directa o indirectamente en una contraprestación de un contrato. Las Directrices citadas anteriormente reconocen una elección real si el responsable del tratamiento ofrece a los interesados una elección entre un servicio con uso de datos para fines adicionales y un servicio equivalente sin tal uso. Aunque no está explicitado, se podría pensar en un servicio remunerado sin publicidad como ejemplo de un servicio equivalente.

Las Directrices dan un ejemplo que evalúa si el consentimiento ha sido manifestación de voluntad libre: Una aplicación de edición de fotografías pide a sus usuarios activar su localización GPS e indica que sus datos serán utilizados para fines de publicidad comportamental. La aplicación no puede utilizarse sin dar consentimiento para el tratamiento a estos fines. Ya que ni la geolocalización ni la publicidad son necesarias para la prestación del servicio (que es la edición de fotografías), pero se impone el consentimiento al uso de los datos a estos fines, se considera que el consentimiento no ha sido prestado libremente. Se estima que el mismo razonamiento sería aplicable a redes sociales que exigen en sus condiciones generales a los usuarios dar consentimiento al uso de datos personales para fines de publicidad comportamental, sin posibilidad de negar tal uso. No se puede hablar de una voluntad libre si el interesado no ha tenido verdadera elección ni control sobre el uso de sus datos y el tratamiento de los datos no es necesario para la prestación del servicio.

La LOPDGDD trata del consentimiento del afectado en su artículo 6 y repite la definición del RGPD en el artículo 6.1. Clarifica en su apartado 2 que, si se pretende tratar los datos para una pluralidad de finalidades, debe desprenderse de manera específica e inequívoca que el consentimiento se da para todas ellas. El apartado 3 del artículo 6 retoma el concepto del artículo 7.4 RGPD y lo parafrasea, estableciendo

que la ejecución de un contrato no puede supeditarse al consentimiento «*para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual*».

2. Ejecución de un contrato con el interesado

La licitud del tratamiento puede surgir cuando es necesario para la ejecución de un contrato con el interesado (artículo 6.1.b RGPD). El Comité Europeo de Protección de Datos adoptó en 2019 unas *Directrices sobre el tratamiento de datos personales en virtud del artículo 6.1.b del RGPD en el contexto de la prestación de servicios en línea a los interesados*. Las Directrices enfatizan la importancia de distinguir el concepto de aceptar condiciones generales para concluir un contrato del hecho de dar consentimiento según el artículo 6.1.a del RGPD. El documento evoca la importancia de cumplir con el principio de limitación de finalidad y de identificar claramente los fines del tratamiento. El tratamiento de los datos debe ser objetivamente necesario para la ejecución del contrato, no siendo posible esta sin el tratamiento de los datos personales en cuestión. Por ejemplo, una persona hace compras en línea y quiere pagar los productos con tarjeta de crédito. El vendedor debe tratar la información de la tarjeta para fines de pago y, por lo tanto, puede apoyarse en el artículo 6.1.b del RGPD como fundamento jurídico para este tratamiento.

Respecto a la posibilidad de utilizar el artículo 6.1.b RGPD como base jurídica para el tratamiento de datos a efectos de enviar publicidad comportamental, las Directrices confirman lo que estableció un Dictamen anterior del Grupo de trabajo del artículo 29³⁰: «*[la necesidad contractual] no es un fundamento jurídico apropiado para elaborar un perfil de los gustos y las opciones de estilo de vida del usuario, basado en su recorrido por un sitio web y en los artículos adquiridos. Ello se debe a que el responsable del tratamiento de los datos no ha sido contratado para elaborar perfiles, sino para entregar bienes y ofrecer servicios concretos, por ejemplo.*»

³⁰ GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*, WP 217, 2014.

Sigue explicitando que, en general, el tratamiento de datos personales con fines de publicidad comportamental no es necesario para la ejecución de un contrato de servicios en línea. Además, subraya que los datos personales no pueden considerarse mercancía comercializable, ya que la protección de datos es un derecho fundamental, amparado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

3. Intereses legítimos perseguidos por el responsable del tratamiento

El artículo 6.1.f RGPD permite el tratamiento si es necesario para satisfacer *«intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales [...]»*. En otras palabras, requiere una prueba de sopesamiento que pondere los intereses legítimos del responsable del tratamiento (o de un tercero) en relación con los intereses o los derechos y libertades fundamentales del interesado. El considerando 48 del RGPD indica que para realizar esta ponderación deben tenerse en cuenta las expectativas razonables del interesado y si este puede prever razonablemente el tratamiento de sus datos. Además, las expectativas dependerán de su relación con el responsable, como por ejemplo cuando el interesado es cliente o está al servicio del responsable. Finalmente, precisa que el tratamiento *«con fines de mercadotecnia directa puede [el subrayado es nuestro] considerarse realizado por interés legítimo»*.

El Grupo de trabajo del artículo 29 publicó en 2014 un *Dictamen sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*. Aunque este Dictamen se refiere a la Directiva 95/46/CE, que fue derogada por el RGPD, el documento sigue siendo válido en su mayor parte, ya que la base jurídica del interés legítimo, ya presente en la Directiva, ha sido sujeta a cambios más bien insignificantes en el RGPD que no afectan a su contenido de manera decisiva para nuestro análisis. Efectivamente, los documentos de orientación adoptados cuando el RGPD ya estaba en vigor remiten

frecuentemente a dictámenes y directrices adoptados por el Grupo de trabajo del artículo 29 con anterioridad al RGPD.

El Dictamen citado anteriormente señala que el concepto de interés legítimo puede comprender una amplia gama de intereses y que el interés debe ser real y actual, lícito y estar articulado con claridad suficiente. Da como ejemplo de un interés legítimo el conocer las preferencias de sus clientes para personalizar mejor sus ofertas, siempre que se prevean garantías adecuadas. Sin embargo, sigue explicando que no es posible utilizar el interés legítimo como base jurídica *«para supervisar de manera indebida las actividades [...] de sus clientes, combinar enormes cantidades de datos sobre ellos [...] y crear [...] perfiles complejos de las personalidades y preferencias de los clientes sin su conocimiento [...]»*, ya que la elaboración de perfiles es una práctica intrusiva y deben prevalecer los intereses y derechos de los interesados.

En lo que se refiere a los intereses o los derechos y libertades fundamentales del interesado, estos deben interpretarse de manera amplia y no son restringidos a intereses legítimos.

Cuando se haya constatado que el responsable tiene un interés legítimo, se procede a la ponderación de los derechos en conflicto. Para realizar dicha prueba, es necesario tener en cuenta un número de factores:

- La naturaleza y fuente del interés legítimo y si el tratamiento es necesario para perseguir dicho interés;
- El impacto sobre los interesados, p. ej. la naturaleza de los datos, la manera en la que se tratan, las expectativas razonables del interesado y la posición del responsable así como del interesado;
- Las garantías adicionales, p. ej. la minimización de datos, técnicas de anonimización, aumento de transparencia y derecho de oposición al tratamiento.

El Anexo 2 del Dictamen enumera una serie de ejemplos para ilustrar la aplicación de la ponderación de los derechos en conflicto, de los que resulta que el artículo 6.1.f del RGPD no es una base jurídica adecuada para el tratamiento de datos con fines de publicidad en redes sociales. Destacamos el ejemplo del organismo sin

ánimo de lucro dedicado al desarrollo humano y social que realiza actividades de recaudación de fondos. A este fin recopila datos de las redes sociales (p. ej. *likes* y contenidos compartidos) y envía mensajes y boletines personalizados a sus miembros, basados en sus interacciones en las redes sociales. El Grupo de trabajo del artículo 29 opina que ese tratamiento excede las expectativas razonables de los afectados por la cantidad de datos recopilados, la falta de transparencia y la reutilización de datos inicialmente publicados con un fin diferente.

Otro ejemplo de alta relevancia es la empresa de Internet que presta servicios de motor de búsqueda, intercambio de videos y redes sociales. Según su política de privacidad, puede «combinar toda la información personal» recopilada sobre sus usuarios a través de los distintos servicios con el fin de «garantizar la mejor calidad posible del servicio». Lo hace sin definición de un periodo de retención de datos. Sin embargo, la empresa facilita a sus usuarios algunas herramientas para ejercer sus derechos, como la posibilidad de desactivar la publicidad dirigida u oponerse a determinados tipos de cookies. Según el Grupo de trabajo del artículo 29, estas herramientas no son suficientes para que los usuarios puedan controlar las combinaciones específicas de sus datos a través de los distintos servicios, y falta la posibilidad de oponerse a la combinación de los datos. Concluye constatando un desequilibrio entre el interés legítimo de la empresa y la protección de los derechos fundamentales de los usuarios.

En los dos casos mencionados, el Grupo de trabajo del artículo 29 concluye que el interés legítimo no puede utilizarse como base jurídica del tratamiento y que el consentimiento sería una base jurídica más apropiada.

Es relevante señalar que el RGPD concede al interesado el derecho a oponerse en todo momento al tratamiento de sus datos cuando tiene por objeto la mercadotecnia directa (artículo 21.2 RGPD). El responsable debe comunicar dicho derecho al interesado explícitamente. La mercadotecnia directa comprende gran parte de la publicidad comportamental dirigida en las redes sociales.

4. Elaboración de perfiles y decisiones individuales automatizadas

El RGPD prevé un número de disposiciones para garantizar que la elaboración de perfiles y las decisiones individuales automatizadas no van en detrimento de los derechos de la persona. Estas disposiciones se aplican también a la recogida de datos para la creación de perfiles, no únicamente a decisiones adoptadas como resultado de la elaboración de perfiles.

El artículo 4.4 RGPD define 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, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física»*. Requiere cierta forma de tratamiento automatizado, aunque no debe ser exclusivamente automatizado, a diferencia del artículo 22 (como se verá más adelante).

La elaboración de perfiles tiene como objetivo evaluar aspectos personales para, habitualmente, asignar la persona a una determinada categoría según sus intereses, su comportamiento u otros parámetros, por ejemplo, para mejorar la segmentación del mercado con fines de mercadotecnia y publicidad³¹.

Cabe recordar que el interesado goza de un número de derechos de información y de acceso a sus datos personales, que incluyen en el caso de elaboración de perfiles tanto los datos utilizados para crear el perfil como los datos sobre el propio perfil y los segmentos a los que se ha asignado al interesado (artículos 13-15 RGPD). El derecho de rectificación según artículo 16 RGPD también es de gran importancia en este contexto, ya que datos inexactos o incompletos pueden llevar a conclusiones o predicciones erróneas sobre la persona³².

³¹ GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, WP251rev.01, 2018.

³² Ibid.

Cuando el tratamiento de los datos personales tiene por objeto la mercadotecnia directa, incluida la elaboración de perfiles, el interesado goza del derecho incondicional de oponerse al tratamiento de sus datos cuando esté relacionado con la citada mercadotecnia. En este caso, el responsable debe dejar de tratar los datos para estos fines (artículo 21 RGPD). Además, el interesado debe ser informado por el responsable de su derecho de oposición en el momento en que se obtengan los datos personales, o en el momento indicado en artículo 14.3 RGPD si los datos no se han obtenido directamente del interesado, dentro de un plazo máximo de un mes a partir del momento en el que se han obtenido los datos.

Las decisiones automatizadas, en cambio, capturadas en el artículo 22 RGPD, pueden derivar de la elaboración de perfiles, mientras que la creación de perfiles puede resultar de decisiones automatizadas, pero son dos conceptos diferentes. El Grupo de trabajo del artículo 29 interpreta el artículo 22.1 RGPD como prohibición general³³ de «*ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él [el interesado] o le afecte significativamente de modo similar*».

Sin embargo, se encuentran excepciones a esta norma, señaladamente si la decisión es necesaria para la conclusión o ejecución de un contrato, si está autorizada por ley o si hay consentimiento explícito del interesado (artículo 22.2 RGPD). Cuando se aplica una de estas excepciones, deben existir siempre medidas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. En particular, el interesado tiene derecho a expresar su punto de vista, a obtener una intervención humana y a impugnar la decisión (artículo 22.2 y 22.3 RGPD). Además, el interesado debe recibir información de que se está realizando una decisión automatizada, así como información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas del tratamiento (artículos 13 y 14 RGPD).

El artículo 22 RGPD se aplica solo a decisiones que entrañan efectos con graves consecuencias (efectos jurídicos o los que afectan al interesado significativamente de modo similar). La publicidad dirigida basada en la elaboración

³³ Ibid.

de perfiles puede tener un efecto suficientemente importante, que debe valorarse caso por caso, teniendo en cuenta factores diversos, como el nivel de intrusión y el seguimiento de las personas en diferentes sitios web, dispositivos y servicios, la forma en la que se presenta el anuncio y el uso de conocimientos sobre las vulnerabilidades de los interesados³⁴. Tales efectos pueden darse en particular en la elaboración de perfiles políticos y el envío de propaganda electoral basada en estos perfiles.

IV. TRATAMIENTO DE DATOS PERSONALES RELATIVOS A OPINIONES POLÍTICAS Y ENVÍO DE PROPAGANDA ELECTORAL

El RGPD prohíbe con carácter general el tratamiento de categorías especiales de datos personales, también llamados «datos sensibles». Explica en su artículo 9 que los tipos de datos personales que se clasifican como «sensibles» son los *«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 las orientación [sic] sexuales de una persona física»*.

Los datos de categoría especial incluyen también datos inferidos de datos que no pertenecen a esta categoría originariamente, pero que entran en ella cuando son combinados con otros datos³⁵. Recordemos el análisis basado en la utilización del botón «Me gusta» en Facebook que reveló datos personales sensibles y podría predecir con un grado de precisión del 85% las opiniones políticas de los usuarios.

El artículo 9 establece una serie de excepciones que permiten el tratamiento de dichos datos, de las que se analizarán únicamente las más relevantes para este trabajo: i) el consentimiento explícito del interesado; ii) datos que el interesado ha

³⁴ Ibid.

³⁵ GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, WP251rev.01, 2018.

hecho manifiestamente públicos; iii) razones de interés público esencial sobre la base de una ley. Otras circunstancias que permiten el tratamiento de datos sensibles son, por ejemplo, obligaciones en el ámbito del Derecho laboral, la protección de intereses vitales o fines de medicina preventiva o laboral. El RGPD reconoce un margen de maniobra a los Estados miembros para especificar sus normas en cuanto al tratamiento de los datos sensibles, como lo indica su considerando 10.

Cabe mencionar que las excepciones del artículo 9 RGPD deben ser aplicadas cumulativamente a las condiciones del tratamiento del artículo 6. Así, el considerando 51 del RGPD indica ya que, además de los requisitos específicos del artículo 9, deben aplicarse los principios generales y otras normas del RGPD, «sobre todo en lo que se refiere a las condiciones de licitud del tratamiento [título del artículo 6]». El Grupo de trabajo del artículo 29 ha confirmado que, para tratar datos sensibles, se debe cumplir con una de las condiciones previstas en el artículo 9, así como una condición del artículo 6³⁶.

En las categorías especiales de datos personales destacan las opiniones políticas que forman el núcleo de nuestro análisis.

1. Consentimiento explícito del interesado

La primera excepción en el artículo 9.2.a RGPD que permite el tratamiento de los datos sensibles es el consentimiento explícito del interesado. Dado que el RGPD ya elevó los requisitos para el consentimiento «normal», se pregunta qué exigencias adicionales hay que observar para el consentimiento explícito. El RGPD no define el consentimiento explícito, pero las *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* del Grupo de trabajo del artículo 29 dan algunas pautas y ejemplos: El consentimiento explícito requiere una declaración expresa de consentimiento, que puede ser mediante confirmación escrita firmada para dar prueba del consentimiento prestado. Valen también otros modos de consentir explícitamente, por ejemplo, rellenando un impreso electrónico, enviando un correo electrónico o mediante casillas de Sí y No incluido el texto «Yo, consiento el tratamiento de mis datos». Podría también existir un sistema de verificación del

³⁶ Ibid.

consentimiento en dos fases, por ejemplo, consentir mediante un correo electrónico de respuesta y después confirmarlo con un código de verificación enviado por SMS. También las declaraciones verbales pueden constituir un consentimiento explícito válido, pero puede resultar difícil comprobar que se han cumplido todas las condiciones necesarias.

Sin embargo, el RGPD admite la posibilidad que el Derecho de la Unión o de los Estados miembros establezca que la prohibición del tratamiento no puede ser levantada mediante consentimiento explícito del interesado. El legislador español se valió de esta posibilidad y dispone en el artículo 9.1 de la LOPDGDD que *«el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico»*. No obstante, se pueden tratar estos datos si se aplica otro supuesto de excepción del artículo 9.2 del RGPD. Se atiende a la formulación divergente del RGPD en cuanto a las categorías de datos sensibles. Así, por ejemplo, el artículo 9.1 de la LOPDGDD no menciona las opiniones políticas, sino la ideología. Además, no menciona los datos genéticos, biométricos y los relativos a la salud, para los cuales existe un régimen especial en otras leyes.

Aunque la ideología y las opiniones políticas no pueden equipararse plenamente, los dos conceptos están estrechamente relacionados. En este sentido, la opinión política puede ser no solo un dato concreto, sino también el resultado de una variedad de datos de los que se puede inferir la ideología de una persona. Como estableció la AEPD en su resolución 02762/2015, la ideología, por su parte, *«puede hacer referencia a ideas o creencias aisladas del individuo»* así como al conjunto de ideas e incluye tanto las que apoya como las que rechaza.

2. Datos que el interesado ha hecho manifiestamente públicos

Otro supuesto de excepción previsto en el artículo 9.2.e RGPD es el tratamiento de datos personales sensibles que el interesado ha hecho manifiestamente públicos. Un ejemplo podría ser un usuario de Facebook que ha configurado su perfil para que sea visible públicamente. Otro ejemplo son los Tweets

en Twitter que están configurados como públicos de manera predeterminada. Sin embargo, no significa que así se pierda el derecho a la protección de sus datos y deben respetarse todos los demás principios del RGPD igualmente. Los datos siguen siendo datos personales y su tratamiento exige las garantías adecuadas, como, por ejemplo, sobre la lealtad, transparencia e información. Como ya se ha mencionado anteriormente, la presencia de una circunstancia del artículo 9 RGPD no es suficiente para tratar las categorías especiales de datos, sino que se requiere adicionalmente el cumplimiento de una condición de licitud del artículo 6 RGPD, puesto que el artículo 9 RGPD no constituye una base jurídica por sí mismo, sino que comprende una serie de excepciones a la prohibición del tratamiento de los datos sensibles. Además, no se prevé un supuesto en el artículo 6 RGPD que permita el tratamiento de datos personales que se hayan hecho manifiestamente públicos y sería absurdo si pudiera justificarse de esa manera el tratamiento de los datos sensibles, pero no de los datos personales «normales» que se han hecho públicos.

3. Razones de interés público esencial sobre base de una ley

Otra circunstancia que levanta la prohibición del tratamiento según el artículo 9.2.g RGPD es si dicho tratamiento *«es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»*. El RGPD hace referencia al concepto de interés público en varios de sus preceptos, pero sin definirlo ni especificar cómo se caracteriza la esencialidad de tal interés. Por lo tanto, incumbe al legislador (nacional o europeo) definir el interés público, así como aclarar su esencialidad. Además, la ley a nivel europeo o nacional que determina este interés público esencial también debe especificar las medidas adecuadas para proteger los intereses y derechos fundamentales del interesado, respetando el núcleo del derecho a la protección de datos. El legislador español hizo uso de esta habilitación e introdujo en la disposición final tercera de la LOPDGDD un nuevo artículo 58 bis a la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG).

3.1. Artículo 58 bis de la Ley Orgánica del Régimen Electoral General

El artículo 58 bis de la LOREG, introducido por la disposición final tercera de la LOPDGDD, permitió a los partidos políticos en sus actividades electorales la recopilación de datos personales relativos a las opiniones políticas y le confirió la consideración de interés público cuando se ofrecían las garantías adecuadas.

Se estima oportuno reproducir el contenido originario del artículo 58 bis de la LOREG:

«Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.

1. *La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.*

2. *Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.*

3. *El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.*

4. *Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.*

5. *Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»*

La introducción del artículo 58 bis a la LOREG fue originariamente propuesta por el Grupo Parlamentario Socialista con la enmienda 331 en la tramitación del Proyecto de la LOPDGDD con el motivo de «*adecuar el Reglamento a las especificidades nacionales y establecer salvaguardas para impedir casos como el que vincula a Cambridge Analytica con el uso ilícito de datos de 50 millones de usuarios de Facebook para mercadotecnia electoral*». Hubo una polémica sobre el artículo 58 bis de la LOREG, en particular su apartado 1, por la preocupación de que la norma hiciera exactamente lo que pretendía evitar y no impidiera tales casos, sino legalizara

la elaboración de perfiles ideológicos y prácticas como las utilizadas en el caso de Cambridge Analytica.

La enmienda propuesta contenía una referencia al considerando 56 del RGPD, que indica que el tratamiento de datos personales sobre las opiniones políticas puede ser autorizado por razones de interés público, siempre y cuando existan garantías adecuadas y previsto que el funcionamiento del sistema democrático en un Estado miembro exige la recopilación de estos datos en el marco de actividades electorales. En el texto adoptado se suprimió esta referencia.

3.1.1. Posiciones de la AEPD

La AEPD publicó una nota de prensa el 21 de noviembre de 2018, justo antes de la votación del Proyecto de Ley en el Senado, que afirmó que el texto del Proyecto no permitía el tratamiento de datos personales para la elaboración de perfiles basados en opiniones políticas, ni el envío de información personalizada basada en perfiles ideológicos o políticos. Según la AEPD, el texto solo permitía la recopilación de los datos para obtener información que permitiera a los partidos políticos *«pulsar las inquietudes de los ciudadanos con el fin de poder darles respuesta en sus propuestas electorales»*. Subsecuentemente, el Gabinete Jurídico de la AEPD emitió un informe el 19 de diciembre de 2018 sobre la interpretación y aplicación del artículo 58 bis de la LOREG y, basándose en este informe, la AEPD adoptó la Circular 1/2019 de 7 de marzo de 2019.

En los dos documentos citados, la AEPD advierte que el artículo 58 bis de la LOREG debe ser interpretado de manera restrictiva al tratarse de una excepción al tratamiento de los datos sensibles y que no podría amparar tratamientos como el microtargeting. Evoca también la necesidad de interpretar el precepto conforme a la Constitución española y los derechos fundamentales como el derecho a la protección de datos (artículo 18.4), el derecho a la libertad ideológica (artículo 16), la libertad de expresión e información (artículo 20) y el derecho a la participación política (artículo 23).

La Circular 1/2019 contiene 11 artículos para fijar los criterios a los que responde la actuación de la AEPD al aplicar las normas sobre protección de datos. Parece que, con su Circular, la AEPD pretendió compensar los huecos que dejó el

legislador. Clarifica que para el tratamiento de los datos relativos a las opiniones políticas en virtud del artículo 58 bis de la LOREG debe concurrir un interés público esencial conforme al artículo 9.2.b del RGPD y que deben adoptarse las garantías previstas en la Circular. La Circular enumera un amplio elenco de garantías que se consideran adecuadas para el tratamiento de los datos mencionados. La AEPD también aclara en su Circular que únicamente las opiniones políticas libremente expresadas por las personas pueden ser objeto de recopilación, pero no otros datos a partir de los cuales se llegue a inferir la ideología política de una persona mediante tecnologías de tratamiento masivo o la inteligencia artificial. Además, declara inadmisibles tratamientos como el microtargeting y los que aspiran a forzar o desviar la voluntad de los electores. Admite empero la elaboración de perfiles toda vez que son perfiles generales y por categorías genéricas de las que pueden deducirse únicamente patrones de conducta generales de la población de manera agregada.

3.1.2 Sentencia de inconstitucionalidad

Sin embargo, el contenido de la Circular se ha vuelto en su gran parte obsoleto después de la Sentencia del Tribunal Constitucional 76/2019 del 22 de mayo de 2019 que declaró inconstitucional el apartado 1 del artículo 58 bis de la LOREG, impugnado por el Defensor del Pueblo mediante recurso de inconstitucionalidad del 5 de marzo de 2019. El Tribunal Constitucional estimó que se infringió la reserva de ley establecida en el artículo 53.1 de la Constitución Española (CE), en esencia, por no haber previsto la Ley Orgánica 3/2018 las garantías adecuadas y por no haber respetado el contenido esencial del derecho fundamental a la protección de datos del artículo 18.4 CE.

Según el Tribunal, para efectuar el análisis, hay que tener en cuenta la especial sensibilidad de los datos afectados, así como la especial posición constitucional de los sujetos autorizados en recopilarlos. Advierte que el derecho fundamental a la protección de datos consiste en otorgar al individuo un poder de disposición y de control sobre sus datos personales. Pronuncia que el derecho fundamental afectado no es solo el derecho fundamental a la protección de datos personales como tal, sino también como derecho instrumental para la protección de otro derecho fundamental, señaladamente la libertad ideológica.

Los derechos fundamentales no tienen carácter absoluto y pueden ser restringidos por medio de la ley, pero toda injerencia debe ser justificada en la protección de otros derechos o bienes constitucionales y debe ser proporcionada al fin perseguido. Además, requiere una habilitación legal para que los ciudadanos no sean afectados por injerencias estatales no autorizadas y para garantizar legalidad y certeza, o sea la seguridad jurídica.

El Tribunal Constitucional, en el fundamento jurídico 6 de la sentencia, exige además que se establezcan mediante ley garantías adecuadas de tipo técnico, organizativo y procedimental para que los intereses jurídicamente protegibles resulten real, concreta y efectivamente protegidos. Solo con existencia de garantías adecuadas puede respetarse el contenido esencial del derecho fundamental. Estas garantías deben asegurar la transparencia, supervisión y tutela judicial efectiva, así como evitar la recogida desproporcionada de los datos y la utilización para fines distintos de aquellos para los que fueron recogidos. El tipo de garantías exigidas depende del tipo de tratamiento, de la naturaleza de los datos y de los riesgos de abuso y de utilización ilícita.

Fundamentalmente, el Tribunal Constitucional critica el precepto impugnado por tres razones: i) No determinó la finalidad del tratamiento de las opiniones políticas. Únicamente mencionó el interés público de manera genérica, pero sin especificar ese interés que fundamenta la restricción del derecho fundamental y sin establecer claramente sus límites y su regulación. Por tanto, no puede valorarse la legitimidad de la finalidad ni la proporcionalidad de la medida. ii) No determinó reglas precisas sobre los supuestos y condiciones en los que puede restringirse el derecho fundamental a la protección de datos. La mención del «marco de sus actividades electorales» no es una condición suficientemente precisa para conocer la finalidad o el bien constitucional que justifica la limitación del derecho fundamental. iii) No incorporó garantías adecuadas ni remitió expresamente a fuentes externas con rango normativo adecuado. La Circular de la AEPD no puede subsanar la insuficiencia constitucional. No se puede recurrir a la interpretación conforme ya que no existen «*varias interpretaciones posibles igualmente razonables*», sino una insuficiencia de regulación. Una remisión al RGPD tampoco es suficiente ya que este solo establece

garantías mínimas y generales sin fijar expresamente medidas adecuadas y específicas.

Por estas razones concluyó el Tribunal que hubo una *“injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear”*.

V. REDES SOCIALES Y POLÍTICAS DE PRIVACIDAD

Se analizarán a continuación las Políticas de Privacidad de Facebook, Google y Twitter, en particular en lo que concierne al uso de datos sensibles, como las opiniones políticas, y las bases jurídicas en las que se apoyan para tratar estos datos con el fin de proporcionar publicidad personalizada. Conviene mencionar que, durante la elaboración de este trabajo, las tres plataformas analizadas todas anunciaron cambios a sus políticas sobre anuncios de carácter político.

1. Facebook

Facebook, que incluye en su política de privacidad a Instagram, afirma utilizar la información de la que dispone, entre otros fines, para personalizar los anuncios tanto dentro como fuera de sus productos. Con el fin de personalizar los productos, Facebook afirma también utilizar datos de categorías especiales (como las opiniones religiosas o políticas) que el usuario decide facilitar a la empresa y para los cuales ha dado su consentimiento explícito.

Facebook no menciona explícitamente la base jurídica en la que se apoya para el envío de publicidad personalizada. De manera general, indica tratar los datos a su disposición *«para cumplir con intereses legítimos propios (o ajenos), incluido nuestro interés en ofrecer un servicio innovador, personalizado, seguro y rentable a nuestros usuarios y socios, a menos que intereses o derechos y libertades fundamentales tuyos que requieran la protección de datos personales prevalezcan sobre ellos»*³⁷. Además, declara basarse en su interés legítimo para proporcionar comunicaciones de marketing y específica como interés legítimo para este tratamiento de datos su

³⁷ «Política de datos». Facebook. Consultado el: 1 diciembre 2019, 21:42. Disponible en: <https://es-es.facebook.com/privacy/explanation>.

interés de «Promocionar los Productos de las empresas de Facebook y realizar marketing directo»³⁸. Se supone que este supuesto se limita a las comunicaciones de marketing enviadas por Facebook y no comprende la publicidad personalizada enviada por anunciantes terceros.

Facebook indica pedir el consentimiento al usuario para el tratamiento de datos con protecciones especiales (por ejemplo, la creencia religiosa, la ideología política, información sobre la salud, si se comparte esta información en los acontecimientos importantes o los campos del perfil de Facebook), a fin de compartir estos datos con quien el usuario elige y para personalizar el contenido. La empresa se basa también en el consentimiento para tratar los datos que los anunciantes y otros socios proporcionan a Facebook sobre la actividad fuera de los productos de las empresas de Facebook con el fin de personalizar los anuncios mostrados «en dichos productos, así como en los sitios web, las aplicaciones y los dispositivos en los que se utilizan nuestros [de Facebook] servicios publicitarios»³⁹. Otros supuestos para los que Facebook pide el consentimiento al usuario son para compartir con los anunciantes datos que identifican al usuario personalmente (por ejemplo, el nombre o la dirección de correo electrónico), y para recopilar información del dispositivo (por ejemplo, ubicación de GPS, la cámara o fotos).

Facebook permite a sus usuarios configurar y modificar las preferencias sobre los anuncios, por ejemplo, descartar intereses inferidos por Facebook o descartar la utilización de cierta información. Sin embargo, no es posible eliminar completamente la publicidad personalizada en Facebook⁴⁰.

³⁸ «Fundamentos jurídicos para tratar los datos». Facebook. Consultado el: 1 diciembre 2019, 21:02. Disponible en: https://es-la.facebook.com/about/privacy/legal_bases.

³⁹ Ibid.

⁴⁰ «About Facebook Ads». Facebook. Consultado el: 1 diciembre 2019, 21:44. Disponible en: <https://www.facebook.com/about/ads>; «Your ad preferences». Facebook. Consultado el: 1 diciembre 2019, 22:07. Disponible en: https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen.

El 20 de noviembre de 2019⁴¹, Facebook declaró estar analizando diferentes maneras para refinar el enfoque de los anuncios políticos, sin revelar más detalles sobre sus planes. Según artículos en la prensa, una de las opciones contempladas es la de limitar el microtargeting de los anuncios, en particular, aumentando el número mínimo de personas necesario para formar un grupo destinatario de los anuncios políticos de 100 personas a unos pocos miles⁴².

2. Google

Aunque Google explica el funcionamiento de los anuncios a través de sus servicios y proporciona cierta información sobre el tipo de datos utilizados para personalizar anuncios, la información proporcionada en la política de privacidad sobre las bases jurídicas para el envío de publicidad personalizada y los distintos datos sujetos al tratamiento es escasa.

Según la política de privacidad de Google, que se aplica también a YouTube, Google se basa en el interés legítimo para mostrar publicidad y en el consentimiento para proporcionar anuncios personalizados, es decir, basados en los intereses⁴³. Google permite en la configuración de anuncios gestionar las preferencias (por ejemplo, modificar los intereses) y desactivar la personalización de anuncios, tanto para personas con cuenta de Google como sin ella⁴⁴.

⁴¹ Anuncio por Facebook de 20 de noviembre de 2019. *Twitter*. Consultado el: 8 diciembre 2019, 13:03. Disponible en: <https://twitter.com/fbnewsroom/status/1197370313937281024>.

⁴² GLAZER, E. «Facebook Weighs Steps to Curb Narrowly Targeted Political Ads». *The Wall Street Journal*. 21 noviembre 2019. Disponible en: <https://www.wsj.com/articles/facebook-discussing-potential-changes-to-political-ad-policy-11574352887?mod=followfacebook>; ROMM, T., STANLEY-BECKER, I. «Facebook has floated limiting political ads and labeling that they aren't fact-checked, riling 2020 campaigns». *The Washington Post*. 5 diciembre 2019. Disponible en: <https://www.washingtonpost.com/technology/2019/12/04/facebook-has-floated-limiting-political-ads-labeling-they-arent-fact-checked-riling-campaigns/>.

⁴³ «Política de Privacidad». *Google*. Consultado el: 30 noviembre 2019, 21:29. Disponible en: <https://policies.google.com/privacy?hl=es>.

⁴⁴ «Configuración de anuncios». *Google*. Consultado el: 12 diciembre 2019, 17:19. Disponible en: <https://adssettings.google.com/authenticated?hl=es>.

Google prohíbe la utilización de información categorizada como sensible para la orientación de anuncios. Hay tres categorías amplias que Google clasifica como sensibles: dificultades personales, identidad y creencias e intereses sexuales. Según la política de Google, la categoría de identidad y creencias comprende, entre otros, la orientación sexual, la afiliación política, la raza y creencias religiosas. Ilustra la afiliación política con los siguientes ejemplos: ideologías políticas, opiniones políticas, partidos políticos, organizaciones políticas, campañas políticas y participación en el debate político⁴⁵.

El 20 de noviembre de 2019 Google anunció que iba a «*promover aún más la visibilidad de los anuncios electorales*», limitando el microtargeting y permitiendo la segmentación por audiencia de estos anuncios solo por las categorías generales de edad, sexo y ubicación general (nivel de código postal). La política se aplica en la Unión Europea desde finales de 2019. Sigue permitiendo la orientación contextual de la propaganda electoral, como mostrar anuncios a personas según el contenido de la página web que están visitando⁴⁶.

3. Twitter

Twitter distingue en detalle los fundamentos jurídicos para diferentes objetivos de tratamiento y menciona los datos utilizados según tipo de tratamiento.

En primer lugar, Twitter se ampara en el interés legítimo para utilizar inferencias sobre las cuentas (como intereses, edad y género), entre otros, para proveer publicidad. Advierte que el usuario puede revisar y modificar las inferencias en cualquier momento. Indica el interés legítimo también como fundamento jurídico para el objetivo de mostrar publicidad en Twitter a partir de los datos proporcionados

⁴⁵ «Ayuda de Políticas de Google Ads». *Google*. Publicidad personalizada. Consultado el: 30 noviembre 2019, 21:32. Disponible en: https://support.google.com/adspolicy/answer/143465?p=privpol_p13nad&hl=es&visit_id=637107426224050344-3989786838&rd=1.

⁴⁶ SPENCER, C. «An update on our political ads policy». *Google*. 20 de noviembre de 2019. Disponible en: <https://blog.google/technology/ads/update-our-political-ads-policy>.

o recopilados en Twitter y para la publicidad mostrada «*en otros sitios web o aplicaciones móviles a partir de la información recopilada allí, exclusivamente*»⁴⁷.

Menciona que, a tal efecto, se tratan los siguientes datos: información básica de la cuenta; información pública; información de contacto; controles de la cuenta; información de ubicación⁴⁸; interacciones con vínculos; datos sobre cookies; datos de registro; datos de socios publicitarios; datos de terceros y afiliados; e inferencias sobre el usuario, en función de estos datos⁴⁹.

Twitter se basa en el consentimiento del usuario para enviar publicidad personalizada. Define este tipo de publicidad como publicidad mostrada dentro y fuera de Twitter en función de la información recopilada sobre el usuario en Twitter, el resto de las actividades que realiza el usuario en línea y los datos proporcionados por los socios de Twitter. Los datos sujetos a este tratamiento son los mismos mencionados anteriormente con la adición de los siguientes: datos de ubicación precisos; «Twitter para datos web»⁵⁰; dispositivos inferidos que pertenecen al usuario; datos de la libreta de direcciones⁵¹.

Twitter prohíbe en el envío de anuncios la selección de palabras clave que segmentan a categorías sensibles como la raza, la religión, la afiliación o pensamientos políticos, la vida sexual o la salud⁵².

⁴⁷ «Resumen de procesamiento de datos y fundamentos jurídicos». *Twitter*. Consultado el: 1 diciembre 2019, 12:45. Disponible en: <https://help.twitter.com/es/rules-and-policies/data-processing-legal-bases>.

⁴⁸ Sin embargo, para tratar datos de la ubicación precisa se requiere el consentimiento del usuario.

⁴⁹ «Resumen de procesamiento de datos y fundamentos jurídicos». *Twitter*. Consultado el: 1 diciembre 2019, 12:45. Disponible en: <https://help.twitter.com/es/rules-and-policies/data-processing-legal-bases>.

⁵⁰ Twitter declara no recopilar datos de Twitter para sitios web si se considera que dichos datos provienen de navegadores pertenecientes a Estados miembros de la Unión Europea o de la Asociación Europea de Libre Comercio.

⁵¹ «Resumen de procesamiento de datos y fundamentos jurídicos». *Twitter*. Consultado el: 1 diciembre 2019, 12:45. Disponible en: <https://help.twitter.com/es/rules-and-policies/data-processing-legal-bases>.

⁵² «Política de Privacidad de Twitter». *Twitter*. Consultado el: 1 diciembre 2019, 12:58. Disponible en: <https://twitter.com/es/privacy>; «Políticas de segmentación por palabras clave». *Twitter*. Consultado

La empresa facilita al usuario distintas herramientas para configurar la privacidad y para modificar o desactivar anuncios personalizados. El control de los anuncios está disponible para todos, independientemente de si se posee una cuenta de Twitter o no⁵³.

El 30 de octubre de 2019⁵⁴, el CEO de Twitter comunicó la decisión de prohibir todos los anuncios políticos en su plataforma a nivel mundial y el 15 de noviembre de 2019 se publicó la nueva política sobre contenido político. La política se aplica desde el 22 de noviembre de 2019 y prohíbe el contenido político promocionado en Twitter, entendido como «*contenido que hace referencia a un candidato, partido político, funcionario gubernamental elegido o designado, elección, referéndum, medida de votación, legislación, regulación, directiva o resultado judicial*»⁵⁵.

Como puede constatarse, las redes sociales ofrecen distintos grados de transparencia respecto a los fundamentos jurídicos en los que se apoyan para el tratamiento de datos personales de sus usuarios a fin de orientar anuncios publicitarios. También tienen enfoques diferentes sobre la posibilidad de utilizar datos sensibles para orientar anuncios personalizados a los destinatarios.

el: 1 diciembre 2019, 12:35. Disponible en: <https://business.twitter.com/es/help/ads-policies/other-policy-requirements/policies-for-keyword-targeting.html>.

⁵³ «Cómo funcionan los anuncios de Twitter». *Twitter*. Consultado el: 1 diciembre 2019, 12:42. Disponible en: <https://business.twitter.com/es/help/troubleshooting/how-twitter-ads-work.html>; «Nuestro uso de cookies y tecnologías similares». *Twitter*. Consultado el: 1 diciembre 2019, 12:43. Disponible en: <https://help.twitter.com/es/rules-and-policies/twitter-cookies#privacy-options>; «Personalización y datos». *Twitter*. Consultado el: 12 diciembre 2019, 17:33. Disponible en: <https://twitter.com/personalization>.

⁵⁴ Anuncio por Jack Dorsey de 30 de octubre de 2019. *Twitter*. Consultado el: 1 diciembre 2019, 14:02. Disponible en: <https://twitter.com/jack/status/1189634360472829952>.

⁵⁵ «Political content». *Twitter*. Consultado el: 1 diciembre 2019, 13:59. Disponible en: <https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html>; «Political Content FAQs». *Twitter*. Consultado el: 1 diciembre 2019, 14:00. Disponible en: <https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content/political-content-faqs11.html>.

VI. CONCLUSIONES

El presente trabajo ha estudiado la publicidad personalizada dirigida en redes sociales bajo el aspecto de la protección de datos. Ha analizado en particular la orientación de publicidad personalizada basada en datos personales sensibles como las opiniones políticas y las prácticas del microtargeting utilizadas en campañas electorales así como el caso de Cambridge Analytica. Además, ha examinado la posibilidad de tratar datos personales sensibles basándose en el interés público mediante el análisis de la sentencia que declaró inconstitucional el apartado 1 del artículo 58 bis de la LOREG. Por último, ha comparado las políticas de privacidad de Facebook, Google y Twitter en cuanto al tratamiento de datos para orientar publicidad personalizada, incluido la utilización de datos personales sensibles.

Terminamos resumiendo las conclusiones principales que pueden extraerse del análisis realizado en el presente trabajo:

PRIMERA. La base jurídica más adecuada para proporcionar publicidad personalizada o comportamental en redes sociales es el consentimiento del interesado. Este consentimiento al tratamiento de datos personales para fines de publicidad debe haber sido prestado libremente y el interesado debe tener la posibilidad de revocar su consentimiento en todo momento sin sufrir ningún perjuicio.

La necesidad contractual no suele ser una condición apta, ya que en general el tratamiento de datos personales con fines de publicidad comportamental no es necesario para cumplir el objetivo del contrato (que es, por ejemplo, ofrecer una plataforma de intercambio de contenido).

La persecución de intereses legítimos normalmente tampoco puede justificar el tratamiento de datos personales para los fines mencionados, puesto que el envío de publicidad comportamental suele basarse en una gran cantidad de datos recopilados con alto grado de intrusión y falta de transparencia sobre el alcance y los tipos de tratamiento de datos. La ponderación de los intereses del responsable y del interesado va a inclinar la balanza a favor del interesado en cuanto no se ofrezcan

garantías adicionales como mejores medidas técnicas y organizativas de seguridad, un elevado nivel de transparencia, de control y elección por parte del interesado.

SEGUNDA. El envío de publicidad basado en categorías especiales de datos, como la utilización de la ideología en la propaganda electoral proporcionada en las redes sociales, debe cumplir con exigencias elevadas.

Datos personales que revelan las opiniones políticas no pueden ser tratados basándose en el consentimiento explícito, ya que la LOPDGDD no lo permite. Estos datos sensibles podrían ser tratados si el interesado los hubiera hecho manifiestamente públicos y si existiera otra condición de licitud que amparase tal tratamiento (como una ley que permitiera el tratamiento de estos datos, véase p.ej. el apartado 2 del artículo 58 bis de la LOREG). Además, pueden ser tratados cuando es necesario por razones de un interés público esencial, establecido por ley y con medidas adecuadas para proteger los derechos del interesado. El artículo 58 bis de la LOREG no cumplió con estas condiciones.

El Tribunal Constitucional clarificó que las garantías adecuadas deben establecerse o en la misma ley que autoriza el tratamiento o en fuentes externas claramente definidas que posean el rango normativo adecuado con remisión expresa a estas fuentes. Además, la finalidad del tratamiento y el interés público esencial deben ser determinados con precisión suficiente y los supuestos y condiciones en los que puede restringirse el derecho a la protección de datos deben ser regulados pormenorizadamente.

TERCERA. Existe una tendencia a restringir el microtargeting, que puede observarse por varios aspectos. Aunque el Tribunal Constitucional no se pronunció sobre las prácticas del microtargeting, es difícil imaginar cómo tales prácticas podrían ampararse en el interés público esencial y cómo podrían cumplir con las demás exigencias formuladas en la sentencia, particularmente las garantías adecuadas. La AEPD sí se pronunció sobre el microtargeting y declaró inadmisibles tales prácticas en virtud del artículo 58 bis de la LOREG, así como el tratamiento de datos personales para la elaboración de perfiles basados en opiniones políticas.

Además, como puede observarse, las propias redes sociales se apartan de su enfoque en lo que concierne al microtargeting. Twitter prohibió de manera general

la propaganda electoral, Google limitó las posibilidades de microtargeting y Facebook también está pensando implementar cambios en su política respectiva.

Queda por ver si se adoptará un enfoque regulatorio más coherente y sistemático con respecto a la elaboración de perfiles y las prácticas de microtargeting. Sería beneficioso tener normas claras y consistentes que regularan cómo y para qué usos es permisible tratar los datos personales relativos a las opiniones políticas. Sobre todo, es crucial cumplir estándares altos de transparencia: Los interesados deben recibir información adecuada sobre la naturaleza de los mensajes recibidos (p. ej. que son personalizados y están basados en su perfil psicométrico), sobre la identidad del anunciante y sobre la manera de poder ejercer sus derechos.

Hay mucho en juego, como pudo observarse en los últimos años cuando proliferaron prácticas a las que se acusó de influenciar a los votantes de manera indebida, facilitadas por la recopilación masiva de datos personales que revelaron aspectos sensibles sobre las personas.

CUARTA. Al fin y al cabo, las empresas y plataformas digitales son conocidas por encontrar cada vez nuevas formas de hacer uso de los datos personales. Debería incentivarse a dichas empresas a encontrar, de la misma manera, formas innovadoras de devolver el control a los usuarios y eliminar los riesgos que conlleva el microtargeting. Podrían utilizar la tecnología e invertir en nuevos sistemas y modelos de negocio que no se aprovecharan del uso de los datos personales, sino que ofrecieran una elección real al usuario e implementaran los principios de protección de datos adecuadamente.

BIBLIOGRAFÍA

Referencias doctrinales

ADSUARA VARELA, B. «El ‘perfilado ideológico’ de los ciudadanos por los partidos políticos». *El Consultor de los Ayuntamientos*. 2019, núm. III, 77, Sección Crónica.

AGAN, T. *Silent marketing: Micro-targeting*. 2007.

ALEJANDRE, G. M. «Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente». *Anuario Jurídico y Económico Escurialense*. 2019, núm. 52, 125-148.

ALEJANDRE, G. M. «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea». *Anuario Jurídico y Económico Escurialense*. 2017, núm. 50, 13-58.

ARROYO ABAD, B. «El tratamiento de los datos personales con fines políticos y electorales. Reflexiones en torno al nuevo artículo 58 bis de la Ley Orgánica del Régimen Electoral General». *El Consultor de los Ayuntamientos*. 2018.

BARBU, O. «Microtargeting in social media: definitions and ethical issues», *Studia Universitatis Babeş-Bolyai – Ephemerides*. 2013, núm. 2, 83-90.

BARNES, J. «Class and Committees in a Norwegian Island Parish». *Human Relations*. 1954, 7, 39-58.

BODÓ, B., HELBERGER, N., DE VREESE, C. «Political microtargeting: a Manchurian candidate or just a dark horse?». *Internet Policy Review*. 2017, 6(4).

CALDER, A. *Reglamento General de Protección de Datos (RGPD) de la UE: Una guía de bolsillo*. IT Governance Publishing. 2017.

DAVARA FERNÁNDEZ DE MARCOS, L. «Los derechos del interesado en el Reglamento Europeo y en la LOPDGDD ¿Qué hay de nuevo?». *El Consultor de los Ayuntamientos*. 2019, núm. III, 48, Sección Crónica.

DELGADO-IRIBARREN G^a-CAMPERO, M. «Novedades en la legislación electoral ante las elecciones locales de 26 de mayo de 2019». *El Consultor de los Ayuntamientos*. 2019, núm. II, 40, Sección Tribuna / Riesgos.

GARCÍA MAHAMUT, M. R. «Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español». *Teoría y Realidad Constitucional*. 2015, núm. 35, 309.

GONZALEZ DE LA GARZA, L. M. «La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el big data». *Revista De Derecho Político*. 2018, núm. 103, 257-302.

GONZÁLEZ GUERRERO, L. D. «Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros». *Estudios Socio-Jurídicos*. 2019, 21(1), 209-244.

KOSINSKI, M., STILLWELL, D., GRAEPEL, T. «Digital records of behavior expose personal traits». *Proceedings of the National Academy of Sciences*. 2013, 110 (15).

MESSÍA DE LA CERDA BALLESTEROS, J. A. «El tratamiento de los datos personales que el interesado hubiese hecho manifiestamente públicos. Especial atención a las Redes Sociales». *Actualidad Civil*. 2018, núm. 5.

ORTEGA GIMÉNEZ, A., GONZALO DOMENECH, J. J. «Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea». *Revista De La Facultad De Derecho*. 2018, núm. 44.

PAPAKYRIAKOPOULOS, O., HEGELICH, S., SHAHREZAYE, M., MEDINA SERRANO, J. C. «Social media and microtargeting: Political data processing and the consequences for Germany». *Big Data and Society*, 2018.

PARDO IBÁÑEZ, B., TORRICO FRANCO, R. «La (in)necesaria existencia de consentimiento expreso del interesado para el envío de comunicaciones publicitarias». *Diario La Ley*. 2018, núm. 9251, Sección Tribuna.

PIÑAR MAÑAS, J. *Reglamento general de protección de datos*. Madrid: Editorial Reus, 2017.

RADCLIFFE-BROWN, A. R. «On Social Structure». *The Journal of the Royal Anthropological Institute of Great Britain and Ireland*. 1940, vol. 70, núm. 1, 1-12.

RECIO GAYO, M. «Los nuevos y los renovados Derechos en Protección de Datos en el RGPD, así como sus limitaciones». *Actualidad Civil*. 2018, núm. 5.

SUÁREZ-GONZALO, S. «Tus likes ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016». *Quaderns del CAC* 44. 2018, vol. XXI – julio 2018 (27-36).

Resoluciones e informes

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 2/2010 sobre publicidad comportamental en línea*, GT 171, 2010.

IAB EUROPE, *EU Framework for Online Behavioural Advertising*. 2011.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*, WP 217, 2014.

IAB SPAIN, *Libro Blanco de Compra Programática*. 2014.

Resolución 02762/2015 adoptada en procedimiento sancionador de la AEPD 235/2015 de 18 de noviembre de 2015.

EUROPEAN ADVERTISING STANDARDS ALLIANCE, *EASA Best Practice Recommendation on Online Behavioural Advertising*, 2016.

GFK CONSORTIUM. *Behavioural Study on Advertising and Marketing Practices in Online Social Media*. European Commission, 2018.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, WP259 y rev.01, 2018.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, WP251rev.01, 2018.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679*, WP260 rev.01, 2018.

Resolución de archivo de actuaciones de la Agencia Española de Protección de Datos. Procedimiento No: E/01873/2018. De las actuaciones practicadas por la Agencia Española de Protección de Datos ante CAMBRIDGE ANALYTICA, FACEBOOK INC., FACEBOOK IRELAND LIMITED, FACEBOOK SPAIN, S.L., AEPD, 2018.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. *EDPS Opinion on online manipulation and personal data*. Opinion 3/2018, 2018.

AEPD, Gabinete Jurídico. Informe del 19 de diciembre de 2018 sobre la interpretación y aplicación del artículo 58 bis de la LOREG. N/REF: 210070/2018. Disponible en: <https://www.aepd.es/media/informes/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-politicos.pdf>.

AEPD. Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. *Boletín Oficial del Estado*, 11 de marzo de 2019, núm. 60, pp. 22834-22840. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2019-3423>.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, version 2.0, 2019.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Statement 2/2019 on the use of personal data in the course of political campaigns*, 2019.

IAB SPAIN, *Estudio Anual de Redes Sociales 2019*. 2019.

Referencias normativas y jurisprudenciales

Constitución Española, *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, pp. 29313-29424. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>.

Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. *Boletín Oficial del Estado*, 20 de junio de 1985, núm. 147, pp. 19110-19134. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1985-11672>.

Ley 34/1988, de 11 de noviembre, General de Publicidad. *Boletín Oficial del Estado*, 15 de noviembre de 1988, núm. 274, pp. 32464-32467. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1988-26156>.

Ley 3/1991, de 10 de enero, de Competencia Desleal. *Boletín Oficial del Estado*, núm. 10, pp. 959-962. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1991-628>.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. *Diario Oficial de la Unión Europea*, 31 de julio de 2002, núm. 201. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32002L0058>.

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. *Boletín Oficial del Estado*, núm. 287, pp. 49181-49215. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2007-20555>.

Carta de los Derechos Fundamentales de la Unión Europea, *Diario Oficial de la Unión Europea*, 26 de octubre de 2012, núm. 326. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>.

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. *Diario Oficial de la Unión Europea*, 4 de mayo de 2016, núm. 119. Disponible en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294, pp. 119788-119857. Disponible en:

<https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>.

Sentencia de 22 de mayo de 2019, Tribunal Constitucional, Recurso de inconstitucionalidad 1405-2019.76/2019, ECLI:ES:TC:2019:76.

Páginas web

«Política de datos». *Facebook*. Consultado el: 1 diciembre 2019, 21:42. Disponible en: <https://es-es.facebook.com/privacy/explanation>.

«Entrega de anuncios». *Facebook*. Consultado el: 4 noviembre 2019, 16:02. Disponible en:

<https://es-es.facebook.com/business/help/430291176997542?id=561906377587030>.

«Política de Privacidad». *Google*. Consultado el: 30 noviembre 2019, 21:29. Disponible en: <https://policies.google.com/privacy?hl=es>.

«Ayuda de Políticas de Google Ads». *Google*. Publicidad personalizada. Consultado el: 30 noviembre 2019, 21:32. Disponible en:

https://support.google.com/adspolicy/answer/143465?p=privpol_p13nad&hl=es&visit_id=637107426224050344-3989786838&rd=1.

«Configuración de anuncios». *Google*. Consultado el: 12 diciembre 2019, 17:19.

Disponible en: <https://adssettings.google.com/authenticated?hl=es>.

SPENCER, C. «An update on our political ads policy». *Google*. 20 de noviembre de 2019. Disponible en: <https://blog.google/technology/ads/update-our-political-ads-policy>.

«Política de Privacidad de Twitter». *Twitter*. Consultado el: 1 diciembre 2019, 12:58. Disponible en: <https://twitter.com/es/privacy>.

«Políticas de segmentación por palabras clave». *Twitter*. Consultado el: 1 diciembre 2019, 12:35. Disponible en:

<https://business.twitter.com/es/help/ads-policies/other-policy-requirements/policies-for-keyword-targeting.html>.

«Cómo funcionan los anuncios de Twitter». *Twitter*. Consultado el: 1 diciembre 2019, 12:42. Disponible en:

<https://business.twitter.com/es/help/troubleshooting/how-twitter-ads-work.html>.

«Nuestro uso de cookies y tecnologías similares». *Twitter*. Consultado el: 1 diciembre 2019, 12:43. Disponible en:

<https://help.twitter.com/es/rules-and-policies/twitter-cookies#privacy-options>.

«Resumen de procesamiento de datos y fundamentos jurídicos». *Twitter*. Consultado el: 1 diciembre 2019, 12:45. Disponible en:

<https://help.twitter.com/es/rules-and-policies/data-processing-legal-bases>.

«Political content». *Twitter*. Consultado el: 1 diciembre 2019, 13:59. Disponible en: <https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html>.

«Political Content FAQs». *Twitter*. Consultado el: 1 diciembre 2019, 14:00. Disponible en:

<https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content/political-content-faqs11.html>.

Anuncio por Jack Dorsey de 30 de octubre de 2019. *Twitter*. Consultado el: 1 diciembre 2019, 14:02. Disponible en:

<https://twitter.com/jack/status/1189634360472829952>.

«Pujas y subastas». *Twitter*. Consultado el: 4 noviembre 2019, 16:05. Disponible en: <https://business.twitter.com/es/help/troubleshooting/bidding-and-auctions-faqs.html>.

«Personalización y datos». *Twitter*. Consultado el: 12 diciembre 2019, 17:33. Disponible en: <https://twitter.com/personalization>.

«Fundamentos jurídicos para tratar los datos». *Facebook*. Consultado el: 1 diciembre 2019, 21:02. Disponible en: https://es-la.facebook.com/about/privacy/legal_bases

«About Facebook Ads». *Facebook*. Consultado el: 1 diciembre 2019, 21:44. Disponible en: <https://www.facebook.com/about/ads>.

«Your ad preferences». *Facebook*. Consultado el: 1 diciembre 2019, 22:07. Disponible en:

https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen.

Anuncio por Facebook de 20 de noviembre de 2019. *Twitter*. Consultado el: 8 diciembre 2019, 13:03. Disponible en:

<https://twitter.com/fbnewsroom/status/1197370313937281024>.

CAREY-SIMOS, G. «How Much Data Is Generated Every Minute On Social Media?». *WeRSM*. 18 agosto 2015. Disponible en: <https://wersm.com/how-much-data-is-generated-every-minute-on-social-media/>.

«IABpedia. El glosario de términos digitales». *IAB Spain*. Consultado el: 4 noviembre 2019, 16:05. Disponible en: <https://iabspain.es/iab-spain/iabpedia/>.

«Real-Time Bidding (RTB): The Complete Guide». *Smaato*. Consultado el: 12 diciembre 2019, 11:30. Disponible en: <https://www.smaato.com/real-time-bidding/>.

LOKE HALE, J. «More Than 500 Hours Of Content Are Now Being Uploaded To YouTube Every Minute». *Tubefilter*. 7 mayo 2019. Disponible en: <https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute/>.

WONG, J. C. «'It might work too well': the dark art of political advertising online». *The Guardian*. 19 mayo 2018. Disponible en:

<https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy>.

«Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios». *BBC News Mundo*. 24 julio 2019. Disponible en: <https://www.bbc.com/mundo/noticias-49093124>.

«EEUU confirma la multa a Facebook por 5.100 millones de dólares». *El Periódico*. 24 julio 2019. Disponible en:

<https://www.elperiodico.com/es/internacional/20190724/facebook-multas-cambridge-analytica-privacidad-7566810>.

«Facebook pagará una multa de 100 millones de dólares por no informar del caso Cambridge Analytica». *El Mundo*. 24 julio 2019. Disponible en: <https://www.elmundo.es/economia/empresas/2019/07/24/5d3815b1fdddf3a0a8b459d.html>.

«La FTC impone penalidad de \$5 mil millones y nuevas restricciones de privacidad de gran envergadura a Facebook». *Comisión Federal de Comercio protegiendo a los consumidores*. 24 julio 2019. Disponible en:

<https://www.ftc.gov/es/noticias/2019/07/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de>.

ADELANTADO, D. S. «¿Cómo usan los políticos los datos personales que se comparten en Internet?». *Expansión*. 14 abril 2017. Disponible en:

<https://www.expansion.com/economia/politica/2017/04/14/58ed09c746163fae588b45cb.html>.

ANGWIN, J., MATTU S., PARRIS T. «Facebook Doesn't Tell Users Everything It Really Knows About Them». *ProPublica*. 27 diciembre 2016. Disponible en:

<https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>.

BECKETT, L. «Trump digital director says Facebook helped win the White House». *The Guardian*. 9 octubre 2017. Disponible en:

<https://www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising>.

CADWALLADR, C. «Google, democracy and the truth about internet search». *The Guardian*. 4 diciembre 2016. Disponible en:

<https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook>.

HERN, A. «Cambridge Analytica: how did it turn clicks into votes?». *The Guardian*. 6 mayo 2018. Disponible en:

<https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.

LAPOWSKY, I. «Cambridge Analytica Could Have Also Accessed Private Facebook Messages». *wired.com*. 4 octubre 2018. Disponible en:

<https://www.wired.com/story/cambridge-analytica-private-facebook-messages/>.

LEWIS, P., HILDER, P. «Leaked: Cambridge Analytica's blueprint for Trump victory». *The Guardian*. 23 marzo 2018. Disponible en: <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory>.

«Criterio de la Agencia Española de Protección de Datos sobre cuestiones electorales en el proyecto de nueva LOPD». *AEPD*. 21 de noviembre de 2018. Disponible en: <https://www.aepd.es/prensa/2018-11-21.html>.

GLAZER, E. «Facebook Weighs Steps to Curb Narrowly Targeted Political Ads». *The Wall Street Journal*. 21 noviembre 2019. Disponible en:

<https://www.wsj.com/articles/facebook-discussing-potential-changes-to-political-ad-policy-11574352887?mod=followfacebook>.

ROMM, T., STANLEY-BECKER, I. «Facebook has floated limiting political ads and labeling that they aren't fact-checked, riling 2020 campaigns». *The Washington Post*. 5 diciembre 2019. Disponible en:

<https://www.washingtonpost.com/technology/2019/12/04/facebook-has-floated-limiting-political-ads-labeling-they-arent-fact-checked-riling-campaigns/>.

«Online ad money pool gets shallower for those outside the duopoly». *WARC*. 21 de marzo de 2019. Disponible en:

https://www.warc.com/newsandopinion/news/online_ad_money_pool_gets_shallower_for_those_outside_the_duopoly/41839.

BRITO, R. «Brazil fines Facebook \$1.6 million for improper sharing of user data». *Reuters*. 30 diciembre 2019. Disponible en: <https://www.reuters.com/article/us->

[facebook-brazil-fine/brazil-fines-facebook-1-6-million-for-improper-sharing-of-user-data-idUSKBN1YY0VK.](https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/)

«Investigation into data analytics for political purposes». *Information Commissioner's Office*. Consultado el: 27 enero 2020, 11:28. Disponible en : <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/>.

BRITO, R. «Brazil prosecutors open investigation into Cambridge Analytica». *Reuters*. 21 marzo 2018. Disponible en: <https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A>.

«ICO statement: investigation into data analytics for political purposes. 2 mayo 2018». *Information Commissioner's Office*. Consultado el: 19 diciembre 2019, 17:47. Disponible en: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/>.

HOLTON, K., SANDLE, P. «UK investigates Facebook over data breach, to raid Cambridge Analytica». *Reuters*. 20 marzo 2018. Disponible en: <https://www.reuters.com/article/us-facebook-cambridgeanalytica/uk-investigates-facebook-over-data-breach-to-raid-cambridge-analytica-idUSKBN1GW0WX>.

«ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information». *Information Commissioner's Office*. 25 octubre 2018. Disponible en: <https://ico.org.uk/facebook-fine-20181025>.

«Facebook agrees to pay Cambridge Analytica fine to UK». *BBC*. 30 octubre 2019. Disponible en: <https://www.bbc.com/news/technology-50234141>.