ISSN 1982-0496

NUEVAS POSIBILIDADES DEL TRATAMIENTO DE DATOS POR LOS PARTIDOS POLÍTICOS EN LA SOCIEDAD DIGITAL

NOVAS POSSIBILIDADES DE TRATAMENTO DE DADOS PELOS PARTIDOS POLÍTICOS NA SOCIEDADE DIGITAL

NEW POSSIBILITIES OF DATA PROCESSING BY POLITICAL PARTIES IN THE DIGITAL SOCIETY

Margarita Orozco González

Doutora em Direito Privado pela Università degli Studi di Bari. Mestra em Direito dos Negócios e em Consumo e Empresa, ambos também pela Universidade de Granada. Graduada em direito pela Universidade de Granada. Atualmente é contratada para aperfeiçoamento do doutorado na Universidade de Granada, e professora visitante na Università degli Studi di Napoli "Parthenope", além de professora colaboradora na Universitat Oberta de Catalunya.

RESUMEN

Actualmente, los datos personales suponen un activo de incalculable. A día de hoy, la posesión de esa información, incluso aquella incompleta y poco individualizada, además de poder constituir una sustanciosa fuente de ingresos por su venta y cesión, facilita canales de publicidad y permite conocer mejor a los destinatarios de servicios de todo tipo. el uso extensivo e intensivo de la información personal de los ciudadanos sin su consentimiento, con fines puramente electoralistas y de expansión del beneficio del partido que esta estrategia implica, supone un claro riesgo para la tutela del derecho a la protección de datos de los ciudadanos, lo que merece, a nuestro juicio, un análisis de la materia. El acceso y tratamiento de la información por parte de los partidos políticos supone un grave riesgo, pudiendo implicar una clara vulneración de los derechos de los ciudadanos, y suponiendo un evidente peligro para la salud de la democracia de los países. Dar el poder a los partidos de segmentar a la sociedad, amoldar los mensajes y perfilar a los ciudadanos, para poder dar publicidad de sus políticas, promesas electorales, etc., les permite falsear su ideario, y rompe con el debido funcionamiento del sistema democrático.
Palabras-clave: Protección de Datos. Partidos Politicos. Democracia.

RESUMO

Atualmente, os dados pessoais são um ativo incalculável. A partir de hoje, a posse desta informação, mesmo a incompleta e pouco individualizada, para além de poder constituir uma fonte substancial de receitas pela sua venda e

cessão, facilita os canais de publicidade e permite-nos conhecer melhor os destinatários dos serviços de todos os tipos. A utilização extensiva e intensiva de informação pessoal dos cidadãos sem o seu consentimento, para fins puramente eleitorais e para alargar os benefícios partidários que esta estratégia implica, constitui um claro risco para a proteção do direito dos cidadãos à proteção de dados, que merece, em nossa opinião, uma análise do assunto. O acesso e o tratamento da informação por parte dos partidos políticos constituem um grave risco, podendo implicar uma clara violação dos direitos dos cidadãos, constituindo um evidente perigo para a saúde da democracia dos países. Dar aos partidos o poder de segmentar a sociedade, moldar mensagens e traçar o perfil dos cidadãos, a fim de divulgar suas políticas, promessas eleitorais, etc., permite-lhes falsificar sua ideologia e romper com o bom funcionamento do sistema democrático.
Palavras-Chave: Proteção de Dados. Partidos Políticos. Democracia

ABSTRACT

Currently, personal data is an incalculable asset. As of today, the possession of this information, even that which is incomplete and not very individualized, in addition to being able to constitute a substantial source of income for its sale and transfer, facilitates advertising channels and allows us to better know the recipients of services of all kinds. the extensive and intensive use of citizens' personal information without their consent, for purely electoral purposes and to expand the benefits of the party that this strategy implies, poses a clear risk to the protection of citizens' right to data protection, which deserves, in our opinion, an analysis of the matter. Access to and treatment of information by political parties poses a serious risk, and may imply a clear violation of the rights of citizens, and posing an obvious danger to the health of the countries' democracy. Giving parties the power to segment society, shape messages and profile citizens, in order to publicize their policies, electoral promises, etc., allows them to falsify their ideology, and breaks with the proper functioning of the democratic system.
Keywords: Data Protection. Political Party. Democracy

1. CONSIDERACIONES INICIALES

Actualmente, los datos personales suponen un activo de incalculable. A día de hoy, la posesión de esa información, incluso aquella incompleta y poco individualizada, además de poder constituir una sustanciosa fuente de ingresos por su venta y cesión, facilita canales de publicidad y permite conocer mejor a los destinatarios de servicios de todo tipo, amén de hacer posible la creación de perfiles que, desde hace tiempo, permiten conocer una imagen, más o menos definida, del consumidor/usuario. Esa posibilidad, que supone una innegable ventaja, se ha perfeccionado y desarrollado con la llegada de técnicas revolucionarias como el Big Data y la Inteligencia Artificial. De manera muy resumida, el primero permite la captación e interconexión de cantidades ingentes de datos y el tratamiento agregado de éstos, y la consecuente creación de bases de datos, la elaboración

de perfiles, ya muchos más perfeccionados, y la capacidad, incluso, de dilucidar preferencias y prever intereses y conductas personales. Por su parte, la Inteligencia Artificial supone el desarrollo de tecnologías autónomas (en mayor o menor medida) que, partiendo de información/datos pueden interpretar y analizar éstos alcanzando la toma de decisiones automatizadas basadas en los mismos.

De este modo, la combinación y suma de todas estas nuevas tecnologías simplifica enormemente la obtención de datos de cualquiera de nosotros, de inicio totalmente desagregados e independientes (y de cualquier tipo), su tratamiento, llevando a cabo una labor de conexión entre ellos – siendo posible hasta la creación de nuestro perfil, fiel a la realidad - incluso más de lo que uno mismo podría imaginarse –, infiriendo de ahí desde gustos, a costumbres, trabajo, cuestiones relativas a la salud, nivel de ingresos, hasta llegar a aspectos de la esfera más privada de la persona, tales como información sobre su vida íntima, condición y orientación sexual y pensamiento político. Siendo estos últimos, datos considerados sensibles, de acuerdo con la normativa vigente de protección de datos europea y nacional española, merecedores, por ello, de una tutela especial, más estricta.

Como mencionábamos *ut supra*, esta posibilidad resulta del máximo interés para cualquier ente, tanto aquellos de naturaleza pública como privada y, por supuesto, para los partidos políticos. Para estos últimos, supone una innegable oportunidad para, por un lado, poder realizar una segmentación del electorado y adecuar su mensaje, las políticas, posicionamientos y promesas electorales a las preferencias del votante; y, por otro lado, les permite diseñar una publicidad personalizada y dirigida de manera directa a cada ciudadano, empleando medios más efectivos que la tradicional propaganda electoral por vía postal, todo ello enfocado a la captación del voto.

Todo ello, lamentablemente, no constituye una simple visión distópica de nuestra realidad, de hecho, cabe recordar que ya hemos sido testigos de escándalos de este tipo, como el caso de “Cambridge Analytica”. Esta empresa, partiendo del consentimiento dado por aquellos que realizaron su encuesta, accedió a los perfiles de todos sus contactos que figuraban en la red como amigos a pesar de carecer de su consentimiento ni estar siquiera informados de dicho acceso y tratamiento.

Sobre esta materia, el Reglamento europeo de Protección de datos (Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), establece un requisito del consentimiento expreso para la legitimidad del tratamiento, por tanto, mucho más restrictivo que el que contemplaba la normativa hasta ese momento; pero, paralelamente, de manera

sorprendente, sin embargo, se abría la puerta al tratamiento de datos por parte de los partidos políticos, aun teniéndose presente que nos encontramos, en algunos casos, ante datos que requieren una protección reforzada al entrar dentro de la categoría de “sensibles”, especialmente protegidos por la misma norma.

Dicha posibilidad fue recogida y ampliada en nuestro ordenamiento interno, a través de la norma de transposición del Reglamento europeo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), lo que ha determinado, a su vez, una modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG). La gravedad y el hondo calado de la cuestión y la, en nuestra opinión, insuficiente y manifiestamente mejorable regulación de la misma en nuestra norma interna ha requerido un pronunciamiento por parte de la AEPD, así como movilización de doctrina y sectores ciudadanos en busca de vías de protección frente a dichos tratamientos, llegando a dar lugar a la interposición, en 2019, de una cuestión de inconstitucionalidad ante el Tribunal Constitucional por parte del Defensor del Pueblo.

Partiendo de estas premisas, podemos afirmar con total convencimiento que el uso extensivo e intensivo de la información personal de los ciudadanos sin su consentimiento, con fines puramente electoralistas y de expansión del beneficio del partido que esta estrategia implica, supone un claro riesgo para la tutela del derecho a la protección de datos de los ciudadanos, lo que merece, a nuestro juicio, un análisis de la materia.

2. EL MARCO NORMATIVO EUROPEO DE REFERENCIA

El RGPD, como hemos adelantado ut supra, efectivamente supuso un fortalecimiento en la tutela de la protección de los datos personales a nivel europeo, en primer lugar, por tratarse de un instrumento normativo de aplicación directa y uniforme en todo el territorio de la Unión, rompiendo la regulación fraccionaria que existía hasta el momento a nivel nacional en los Estados miembros. En segundo lugar, la norma instaura un blindaje sin precedentes de este derecho, ampliando su objeto y restringiendo los supuestos de obtención y tratamiento legítimos, y extendiendo tanto los derechos ARCO (de acceso, rectificación, cancelación y oposición), con el famoso derecho al olvido, entre otros (junto con el derecho de supresión, portabilidad, a la limitación del tratamiento) , como el ámbito de aplicación de la norma, incluyendo todo tratamiento de datos de ciudadanos

de la Unión llevado a cabo por servicios ofertados en el ámbito europeo[1]. De manera especial, se pone el énfasis en el consentimiento, erradicando con ello a las casillas de aceptación pre-marcadas, de modo que sólo legitima un tratamiento el consentimiento expreso del titular[2], salvo supuestos muy concretos. Se desarrollan, asimismo, dos principios clave, sobre todo en la era de Internet y las *apps*, como son el de "Privacy by design" (o desde el diseño) y "Privacy by default" (o por defecto), que determinan la obligación de predeterminar de origen los mayores niveles de protección de los datos, lo cual se debe contemplar además en el propio diseño de páginas, aplicaciones y servicios en general. En este contexto, manteniendo la esencia de la regulación precedente, se tutelan de manera más estricta, por su naturaleza, una tipología especial de datos, denominados "sensibles". Estos datos, de acuerdo con el artículo 9 RGPD, son los relativos al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como aquellos datos genéticos, biométricos y los relativos a la salud, a la vida sexual o a la orientación sexuales de una persona física. Dicho tratamiento, de acuerdo con el apartado 1 del citado artículo 9, queda prohibido, con la salvedad de una serie de excepciones que recoge en el apartado 2, entre las que cabe destacar, para el tema que nos ocupa, las siguientes: "*El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:*

> a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
> (…)
> c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
> d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de

[1] Art. 3 RGEPD "1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un estable- cimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

[2] Art. 4. 11 RGEPD "«consentimiento del interesado»: 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;"

> tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
> e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
> (…)
> g) el 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; (…)"

Teniendo en cuenta lo anterior, por cerrar el repaso a la norma europea, encontramos en concreto en el Considerando 56 una excepción específica para el caso de los partidos políticos, en la que deja abierta la puerta al legislador nacional para establecer una excepción a la limitación del tratamiento en ese contexto. En el mismo dispone que "*Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas."*

Ambos puntos son claves para el análisis de las cuestiones principales que nos ocupan en la norma española y, específicamente, en el contexto de la obtención y tratamiento de datos por los partidos políticos.

3. LA DEL RÉGIMEN ELECTORAL GENERAL ESPAÑOLA.

A la luz de lo anterior, debemos entender que es esta habilitación, ex Considerando 56 del RGPD, junto con el artículo 9 del mismo RGPD, en la que se basa la norma española de Protección de Datos, la Ley española de Protección de Datos, 3/2018 (LOPDGDD), para recoger en nuestro ordenamiento jurídico la posibilidad de captación y tratamiento de datos por parte de los partidos políticos en el marco de las campañas electorales.

Como punto de partida, debemos señalar que existe cierto debate en la doctrina[3] acerca de la vinculación que los considerandos de un Reglamento europeo puedan tener para los Estados miembros, ya que una parte de la misma sostiene que son meros elementos interpretativos y, para otra si implican una sujeción para el legislador nacional; cuestión que no es baladí en un supuesto como este, en el que, además, el partido político que presentó la enmienda que introdujo dicha posibilidad en la norma española lo justificó

[3] Al respecto, vid. ADSUARA, B. y MARTINEZ, R., "Debate sobre el nuevo artículo 58 bis de la LOREG", LA LEY privacidad, Núm. 1, Wolters Kluwer, 2019.

con la "obligatoriedad" que imponía el Considerando.

Partiendo de ello, en primer lugar, es preciso hacer referencia al artículo 9.1 de la LOPDGDD, el cual, recogiendo la posibilidad dada por el Reglamento en su artículo 9, determina que el tratamiento de datos sensibles no quedará legitimado por el mero consentimiento del titular de los mismos[4]. Admitiendo acto seguido, eso sí, que "*lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda*". Sobre la base de este marco normativo, la Disposición final tercera de la LOPDGDD: **"***Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General"* incorpora en la LOREG un controvertido artículo 58 bis. 1 con la siguiente redacción:

> "**«**Utilización de medios tecnológicos y datos personales en las actividades electorales.»
> (…)
> 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.
> (…)
> 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición."

Aunque no se aclara en el contenido del mentado precepto, debemos entender que dicha habilitación se basa, de entre los supuestos previstos en el artículo 9 del RGPD, bien en el relativo al tratamiento de datos personales que el interesado ha hecho manifiestamente públicos (art. 9.2 e) o el referido al tratamiento que resulta necesario por razones de un interés público esencial (del apartado g) del art.9.2), ya que no entraría dentro del ámbito objetivo de la legitimación recogida en el apartado d), que hace referencia al tratamiento efectuado en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical "*siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados*".

[4] Art. 9 LOPD "1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, 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."

Resulta, no obstante, llamativo, en nuestra opinión, que se permita a un organismo o ente sin ánimo de lucro exclusivamente el acceso a los datos de miembros o ex miembros de las mismas, mientras que a los partidos políticos se les autorice la captación de datos de cualquier ciudadano. Asimismo, resulta complicado aceptar el encuadramiento de las finalidades perseguidas para el tratamiento por un entre privado, como es un partido político, dentro de la idea de interés público, en el sentido contemplado por la normativa; tal concepción implica, en nuestra opinión, una deformación perversa de dicho concepto. Esta opinión coincide con la plasmada por el Supervisor Europeo de Protección de datos, cuando, en su opinión de 2018 sobre la materia, subrayaba que "*en particular, el concepto de interés público en la normativa de protección de datos y cómo difiere de los intereses privados de las empresas y los movimientos políticos es clave para tratar los abusos y manipulaciones que se producen en el espacio político online*"[5].

Llegados a este punto, consideramos relevante detenerse en esa noción de "interés público", ya que, por un lado, observamos que el considerando 56 RGPD introduce un elemento condicional al determinar que "*Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige* (…)*"*, algo que el artículo 58 bis ignora y convierte en afirmación rotunda. Aquí compartimos la opinión de ADSUARA cuando sostiene que "*habría que explicar cuál es el supuesto de hecho que 'exige' que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas para el (buen) funcionamiento del sistema democrático en España. Cuando, más bien al contrario, parece que el buen funcionamiento del sistema democrático 'exige' que no se haga*."[6] Por otro lado, encontramos que la norma no precisa cuál es el interés público esencial que justifica este tratamiento de datos personales, siendo además necesario que justificara la proporcionalidad con respecto al objetivo que se persigue, así como el respeto al derecho a la protección de datos. Unido a ello, se detecta la ausencia total en la misma de cualquier

[5] Traducción de la autora, texto original: "*In particular, the notion of public interest under data protection law and how it is distinct from the private interests of companies or political movements is key to addressing abuses and manipulation occurring in the online political space*" (EDPS Opinion 3/2018, on online manipulation and personal data; pág. 19).

[6] ADSUARA, B., y MARTINEZ, R., op. cit., pág. 5. Se alinea con esta postura SANTOS, defendiendo que "no se justificaba en ningún momento en qué medida el funcionamiento del sistema democrático español, cuyo 40 cumpleaños se estaba celebrando en ese momento, exigía que los partidos políticos recopilaran datos personales sobre las opiniones políticas de las personas cuando, precisamente, a nivel internacional se está siguiendo la línea opuesta." (SANTOS SANCHEZ, D. J., "Comentario del Informe 2018-0181 y la Circular 1/2019 de la AEPD, sobre tratamiento de datos relativos a opiniones políticas por partidos políticos", La Ley Privacidad, núm. 1, 2019, pág. 3)

mención a medidas adecuadas y específicas y garantías tendentes a proteger los intereses y derechos fundamentales del interesado, como se exige en el art. 9.2.g del RGPD.

Otro punto crítico que hemos de subrayar es el relativo a la discordancia que supone el hecho de que el legislador español optara por no hacer uso de la excepción, que contemplaba el Reglamento, a la prohibición de tratamiento de datos sensibles en los casos en que medie el consentimiento del titular, para, sin embargo, acto seguido, permitir un acceso y uso de éstos por los partidos políticos. Es cierto que en plena era digital resulta necesaria la introducción de la tecnología en el proceso electoral, pero resulta un contrasentido estructurar un blindaje amplio a este derecho fundamental, para crear paralelamente un extenso espacio de desprotección en este ámbito.

Esta problemática, interesa subrayar, se da en el caso de datos ideológicos, los cuales, según la Sentencia de la Audiencia Nacional de 28 de septiembre de 2001, serán "cualquier dato que sirva para identificar a una persona que pueda poner de manifiesto su perfil ideológico o de otra índole". Serían estos, por tanto, los que integrarían la previsión que nos ocupa. Empero, a modo de apunte, también existe un debate en cuanto a qué tipo de datos constituyen el elemento objetivo de esta habilitación al tratamiento ya que, como apunta ARROYO[7], si la finalidad del art. 58 LOREG, tal y como afirma la AEPD es la utilización de opiniones anónimas exteriorizadas libremente buscando "*pulsar el estado general de la ciudadanía en el espíritu de integrar sus propuestas programáticas y mandar propaganda electoral, no era preciso reformar nada, porque el marco legal existente ya lo permitía sin necesidad de calificar de interés público o general la operación de tratamiento de datos sensibles realizado por partidos políticos, lo que son palabras mayores*"[8]. Sin embargo, coincidiendo con el citado autor, defendemos que este, claramente, no es el ánimo del artículo en cuestión dado que, como se desprende de éste, legitima el tratamiento de "datos personales relativos a opiniones políticas de las personas", haciendo referencia, por tanto, de manera evidente, a opiniones difundidas por un sujeto en una red social, foro o portal web, tratándose de "*información que sitúa al individuo en un determinado entorno*

[7] 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,* Editorial Wolters Kluwer, 2018; pág. 8.

[8] Ello, concuerda con lo concluido por la AN en su jurisprudencia reiterada, en sentencias de 4 de abril de 2014, siguiendo la doctrina de la ST de 29 de abril de 2009, donde se dispone que "*las opiniones, comentarios o manifestaciones realizados sobre o por un persona no pueden considerarse datos personales y deben quedar al margen del ámbito de aplicación de la LOPD (hoy LOPDGDD) por cuanto no revelan datos personales de la misma*."

social, laboral o espacial que determina un posicionamiento ideológico, en el que se pretende actuar e influir"[9].

Por otro lado, sensu contrario, el tratamiento por estos entes de datos que no revistan la categoría de sensibles, como podría ser un número de teléfono, el perfil en una red social, la dirección de correo electrónico, etc., podría quedar amparado en el supuesto recogido en el art. 6.1. f) del RGPD, que legitima su utilización en el contexto de que el "*tratamiento* [sea] *necesario para la satisfacción de 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 particular cuando el interesado sea un niño*." Al respecto, es importante reseñar que el carácter aparentemente más genérico de estos datos permite, a través del recurso a las ciencias del comportamiento, inducir rasgos de la personalidad del sujeto; así lo defienden KALTHEUNERM y BIETTI[10], quienes demuestran que solo a través de la información que da la forma de pulsar un teclado de ordenador o, aún con mayor precisión, la de un dispositivo táctil, puede revelar cuestiones inherentes al estado psíquico-emocional de la persona tales como nivel de confianza, nerviosismo, tristeza o cansancio, cuestión, no obstante, sobre la que volveremos más adelante.

Una cuestión a puntualizar, asimismo, es la indeterminación del concepto de datos hechos manifiestamente públicos, ya que surge inevitablemente la duda de cuál debe ser el público objetivo de dicha comunicación: ¿entra dentro del ámbito objetivo de esta previsión, por ejemplo, una cuenta con acceso limitado a determinados sujetos en una red social?, ¿Qué debemos considerar en concreto por fuente de acceso público?[11].

En este punto, resulta interesante reseñar que, de forma expresa, las autoridades de protección de datos de Italia y Francia[12] determinaron respectivamente, en 2014 y 2016,

[9] ARROYO ABAD, B., Op. Cit.; pág. 8

[10] KALTHEUNER, F., BIETTI, E., "Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR", J*ournal of Information Rights, Policy and Practice* (IRP&P), Winchester University Press, 2018; págs. 3-4

[11] Un análisis de esta cuestión se llevó a cabo en OROZCO GONZALEZ, M., "La utilización ilícita de datos de carácter personal por los partidos políticos", Actualidad civil, núm. 7, 2021.

[12] Vid. "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" published in the Official Gazette of the Italian Data Protection Authority number 71 on 26.03.2014 [doc. web n. 3013267]. Fuente: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 y "Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?" published by the Commission Nationale de l'informatique et des libertés (French National Commission of Informatics and Liberty) 08.11.2016. Fuente: https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux

de forma diametralmente opuesta a las de España, la prohibición de la información hecha pública por el sujeto sin ninguna conexión con estos fines, habilitándose exclusivamente esa captación, en el caso francés, cuando media el consentimiento del titular.

Volviendo a nuestro país, conforme a la interpretación literal del artículo 58 bis LOREG, la conclusión que se extrae es que legitima la captación y tratamiento de datos de carácter personal de cualquier tipo[13] – ya que no se recoge ninguna excepción para tipologías especiales como son los datos sensibles – y con independencia del medio, siempre que se obtengan de cualquier fuente pública, en concreto páginas web (¿debemos entender, por tanto, dentro de ellas foros y portales como Twitter?), pero de manera general cualquiera de acceso público. Además, no se clarifica el contexto o marco en que se podrá llevar a cabo el tratamiento, al incluir el precepto un lacónico marco de "actividades electorales", lo que no permite concluir si esta recopilación de opiniones políticas vinculadas a datos personales sólo podrán hacerla durante la campaña electoral oficial o se trata de un contexto más amplio. *Concreta*, asimismo, que los partidos políticos podrán utilizar dicha información para la realización de "actividades políticas" durante el período electoral, lo que constituye un cajón de sastre para un amplísimo abanico de usos, indeterminación absoluta que, a nuestro juicio, resulta inaceptable dentro del régimen jurídico sentado por el Reglamento europeo y nuestra Constitución, por la inseguridad jurídica que genera.

Unido a ello, el único requisito que se deduce del precepto, en principio, es el de informar debidamente al titular de los datos de la posibilidad de ejercitar el derecho de oposición, pero se abren múltiples dudas: ¿la información no debería referirse también al derecho de supresión o derecho al olvido?, y ¿por qué vía se debería suministrar esta información?, ¿bastaría con un mensaje publicado en un portal web o debería hacerse por el mismo medio en el que se ha obtenido la información?; ¿a quién debe dirigirse?; ¿no se exige la inclusión de la información sobre la persona física o jurídica competente para su recepción y gestión?.

Vinculado a lo anterior, echamos en falta una mención específica a los deberes de información, en sentido general, que el RGPD establece en esta materia para el responsable, constituyendo un pilar fundamental de la regulación actual de la protección de

[13] Lo cual permite afirmar, como hace ADSUARA, que "*Los partidos políticos podrán llevar a cabo la recopilación de datos personales relativos a las opiniones políticas de las personas. O sea, «perfiles ideológicos» de personas identificadas o identificables. Si no, no serían «datos personales».*" (ADSUARA VARELA, B., "El «perfilado ideológico» de los ciudadanos por los partidos políticos", *El Consultor de los Ayuntamientos*, Núm. III, Sección Crónica, Julio 2019, pág. 79.)

datos los principios de transparencia y tratamiento leal.

Conforme a esta argumentación, no encontramos motivos lógicos que avalen que este tipo de utilización justifique la eliminación de todas las garantías y protección que de manera general consagra la norma en el ámbito de los datos personales, por lo que consideramos que, con su admisión, el legislador incurre en una clara contradicción con el espíritu del Reglamento Europeo.

4. NUEVOS RIESGOS: EL PERFILADO DE LOS USUARIOS Y LA CESIÓN DE DATOS A TERCEROS

Otra cuestión preocupante y discutible, ya esbozada en puntos anteriores, es la que se refiere al recurso de técnicas de Big Data e Inteligencia Artificial, así como la elaboración de perfiles, partiendo de la información captada. Especialmente en lo referente a la última, se define por el RGPD (artículo 4.4), 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*". Esta posibilidad es realmente interesante y rentable para los partidos políticos, los cuales, utilizando el Big Data y/o inteligencias artificiales, puede crear perfiles individuales o más genéricos segmentando a grupos de población en base a diversos criterios, algo muy peligroso en la práctica, pero también muy beneficioso para estas entidades.

Estas posibilidades se expanden aún más por vía de la utilización de los modernos sistemas inteligentes (del tipo "Alexa", "Echo" y similares), que, con sus facultades de escucha e interpretación, mediante tecnologías de IA, obtienen valiosa información sobre los hábitos diarios de sus usuarios e, incluso, mediante el análisis del tono de voz pueden llegar a evaluar su nivel de pensamiento crítico y capacidades de escucha activa[14]. Todo ello se suma al resto de indicios que se obtienen de manera desagregada del comportamiento de la persona en redes sociales ("me gustas" o "retuitteos"), historiales de búsqueda y distintas fuentes más o menos públicas, algo ya puesto en práctica en las elecciones norteamericanas y en el referendum del Brexit[15].

[14]ALTHEUNER, F. y BIETTI, E., "Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR", *Journal of Information Rights, Policy and Practice*, 2(2), 2018; págs. 4-5.
[15] "Big Data combined with behavioural science enables inferences about even deeper personality portraits. Some data analytics companies specialise in assessing individuals based on five personality traits known as

Es un hecho contrastado que la interpretación conjunta, creando un perfil, de todos estos datos habilita la manipulación de la información que le es mostrada al usuario y con ello la posibilidad de influir en su pensamiento político[16]. Esta influencia, como subraya el Supervisor Europeo de Protección de datos, nos lleva a considerar que "*la personalización automática del mensaje ya prevalente en el ámbito comercial puede, cuando se aplica en la esfera política, en teoría aplicarse a la página web de un partido o candidato político, ajustando su contenido a las preferencias políticas conocidas del visitante. Ello también permitiría la obstrucción de una búsqueda de calidad y de iniciativas de control que persigan analizar cómo los partidos/candidatos mantienen sus promesas electorales una vez alcanzado el poder*"[17]

Al respecto de la creación de perfiles, de acuerdo con el artículo 13 del RGPD, en principio, el responsable del tratamiento estaría simplemente obligado a informar al titular de la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado (art. 13.2. f) y art. 14.2. g) RGDP), tanto cuando la información haya sido obtenida del titular como cuando no sea así.

Tal conducta entendemos podría quedar amparada por el artículo 22.2 del Reglamento por cuanto, en conexión con el apartado 1, que dispone que todo interesado tendrá derecho a no ser objeto de una decisión automatizada, incluida la elaboración de perfiles, que sea susceptible de producir efectos jurídicos en él o le afecte significativamente de modo similar, determinando una excepción en el caso de esté legitimada por el Derecho de la Unión o el nacional de los Estados miembros que sea de aplicación al responsable del tratamiento y *"que establezca asimismo medidas adecuadas para salvaguardar los*

---

the 'Big Five' or OCEAN, using data gathered from online personality tests (see above), a technique reported to have been exploited by campaigners during 2016 US Presidential elections and UK Brexit referendum34. These assessments are then supplemented with additional characteristics, including values and needs, likes and shares35. Profiling serves also to identify other people who might be potentially interested in a product and service, namely the 'lookalike' audience and customers held by the major social media platforms". (EDPS Opinion 3/2018, Op.cit.; pág. 8)

[16] ALLCOTT, H. y GENTZKOW, M., "Social Media and Fake News in the 2016 Election (Spring 2017)", Stanford University, *Journal of Economic Perspectives*, Vol. 31, No. 2, 2017, pp. 211-236; así como ZUIDERVEEN BORGESIUS, F. & TRILLING, D. & MÖLLER, J. & BODÓ, B. & DE VREESE, C. & HELBERGER, N., "Should we worry about filter bubbles?", *Internet Policy Review*, núm. 5(1).

[17] Traducción de la autora. Texto original: "The automatic tailoring of messaging already prevalent in the commercial space could, where applied to the political sphere, in theory involve a political candidate's or party's webpage adjusting its content according to the known political preferences of the visitor. It could also creates obstacles for quality research and accountability initiatives aiming to track how political candidates are holding on to their promises once they are at the office lead to involve" (EDPS Opinion 3/2018, op. cit.; pág. 12)

derechos y libertades y los intereses legítimos del interesado". Y ello, porque el apartado 4 del mismo precepto estipula que "*Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*", de modo que nos encontraríamos ante uno de los supuestos a los que se acoge esta posibilidad.

Así, se concluye que nuestro marco jurídico admite el 'targeting' ("segmentación por categorías genéricas"), con el fin de conocer las opiniones políticas, no así 'microtargeting' ("perfilado personalizado"). Sin embargo, la realidad es que la posibilidad de entrecruzar datos que permite el Big Data, y la capacidad de las IA para aprender de esa información y tomar decisiones en base a ella, facilitan el desarrollo de actividades y conductas enfocadas de manera personalizada a los sujetos, sin haber individualizado per se a éstos[18]. Sobre este punto alerta la Comisión Europea en sus Orientaciones, subrayando que la elaboración de perfiles puede derivar en su uso para seleccionar personas de forma específica, es decir, analizar datos personales, como puede ser el historial de búsquedas en internet de un sujeto, y detectar los intereses particulares de una persona o público específico *"con el fin de influir en sus acciones.*" Como se alerta en las citadas orientaciones, *"la selección muy específica puede utilizarse para dar un mensaje personalizado a una persona o al público utilizando un servicio en línea, por ejemplo, las redes sociales*."

Continuando con la idea, en el contexto específico de las redes sociales, se resalta en el documento que esta problemática se ha puesto de relieve en el caso Cambridge Analytica, donde se ha evidenciado la aplicación de métodos de selección muy específica de sujetos en las redes sociales, mostrando de facto que las organizaciones pueden, o más bien, de hecho, están captando datos de los usuarios de las redes sociales de los usuarios con el objeto de crear perfiles de votantes. El riesgo reside, como determina la Comisión, en que "*esto podría permitir a esas organizaciones identificar a aquellos votantes que*

[18] Tal y como defiende SANTOS, "*el uso de técnicas modernas como el big data, la inteligencia artificial y la aplicación del microtargeting en los procesos electorales pueden llevar a la manipulación de las personas mediante la realización de perfilados exhaustivos y el fenómeno de las «fake-news» o «desinformación online»,* (…)", ello, estamos de acuerdo, demuestra que con la regulación de estas conductas se consigue exactamente el efecto contrario que, según se manifestaba en la enmienda, se perseguía: evitar situaciones como las derivadas de casos como el de Cambridge Analytica. (SANTOS SANCHEZ, D. J., "Comentario del Informe 2018-0181 y la Circular 1/2019 de la AEPD, sobre tratamiento de datos relativos a opiniones políticas por partidos políticos", op. cit; pág. 2

pueden ser más fácilmente influenciables y, por tanto, permitirles influir en el resultado de las elecciones."[19]

La realidad aquí es que aquellas prácticas consistentes en la selección de manera específica en contexto electoral se deben considerar como toma de decisiones automatizadas cuando produzcan efectos suficientemente importantes. De acuerdo con el RGPD, esto ocurre cuando la decisión tiene la potencialidad de afectar significativamente a las circunstancias, comportamiento o decisiones de las personas o tiene un impacto prolongado o permanente sobre las mismas, según destaca el Comité europeo de protección de datos en sus Orientaciones sobre decisiones automatizadas, WP251 rev.01, revisadas por última vez y adoptadas el 6.2.2018. En ellas, el citado Comité consideró que la publicidad personalizada en línea podría ser capaz, en algunas circunstancias, de afectar significativamente a las personas "*cuando, por ejemplo, es intrusiva o aprovecha su conocimiento de aspectos vulnerables de las personas. Dada la importancia del ejercicio del derecho democrático al voto, los mensajes personalizados cuyo posible efecto sea, por ejemplo, que las personas no voten, o voten de una forma específica, podrían potencialmente cumplir el criterio de efecto significativo*." En conclusión, en contexto electoral, los responsables deben garantizar que todo tratamiento que emplee esas técnicas es lícito con arreglo a los citados principios y las estrictas condiciones que marca el Reglamento.

Como último aspecto a tratar en el desarrollo del presente análisis, debe abordarse la problemática cuestión de la cesión a terceros de la información y la posibilidad de encargar a éstos la obtención y tratamiento de la misma. Al respecto, el silencio del precepto conduce a considerar su admisibilidad. Sobre este tema, solo encontramos una referencia, ciertamente detallada, en el ya mencionado documento de Orientaciones de la Comisión Europea sobre protección de datos en el contexto electoral. En las mismas, por un lado, se observa la situación en que el partido político actúa como responsable del tratamiento, previendo aquí que deberá entonces "*comprobar si los datos procedentes de terceros han sido obtenidos legalmente y para qué fines (por ejemplo: si las personas afectadas han dado su consentimiento informado para una finalidad determinada)"* y "*aclarar las obligaciones en los contratos u otros actos jurídicos vinculantes con los encargados del tratamiento de datos, como empresas de análisis de datos*". Pero también, por otro lado,

[19] "Orientaciones de la Comisión Europea relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral", op. cit., pág. 8

se contemplan las situaciones en que los intermediarios y las empresas de análisis de datos sean, bien conjuntamente responsables o bien encargados del tratamiento de los datos, dependiendo del grado de control que tengan sobre el mismo, matizando según el caso los deberes de éstos; así como aquellos en que las plataformas sean las responsables del tratamiento de datos, lo que ocurre cuando este se realiza en sus plataformas y pueden ser corresponsables con otras organizaciones[20].

Este esquema se ha visto refrendado en la praxis judicial en una reciente sentencia de la Audiencia Nacional, de 12 de marzo de 2020, de la Sala de lo Contencioso (rec.157/2018), donde se sostiene que "*le corresponde al responsable dictar al encargado las instrucciones para el tratamiento de datos personales que vaya a realizar en el marco objeto del contrato, por lo que éste debería haber advertido de la necesidad de solicitar el consentimiento expreso y por escrito. Además, sin perjuicio de las responsabilidades que puedan recaer en el encargado, éste actúa siempre por cuenta y en nombre del responsable*." De esta forma, como concluye SEMPERE, "*En consecuencia, hay una falta de diligencia del Ayuntamiento sobre la actuación del encargado que supone el elemento culpable, y por tanto, es responsable de la infracción cometida*."[21] No obstante, en este caso el quid de la cuestión reside una vez más, como sostiene la AN, en el consentimiento del titular, si bien debemos recordar que el artículo 9 de nuestra LOPDGDD no contempla el consentimiento como elemento legitimador para el tratamiento de los datos sensibles, como es el caso de los relativos a la ideología.

La resolución judicial precitada resuelve el recurso interpuesto por el Ayuntamiento de Valencia frente a una Resolución de la AEPD en la que se le imputaba una vulneración del artículo 7.2 de la LOPDGDD por el tratamiento de datos de ideología y religión, sin la preceptiva solicitud previa del consentimiento, expreso, escrito e informado de los afectados[22], en el marco de una encuesta realizada a falleros y comisiones falleras cuya

[20] En este contexto, entre otros deberes, cabe destacar la impuesta de "*elegir la base jurídica adecuada para tratar los datos: contrato con personas, consentimiento, interés legítimo. Si son «datos sensibles», solo es posible tratarlos con el consentimiento explícito o si los datos se han hecho manifiestamente públicos*" (Orientaciones de la Comisión Europea, sobre protección de datos en el contexto electoral, op. cit.; pág. 11 y ss.)

[21] SEMPERE SAMANIEGO, J., "Tratamiento de datos de ideología política y religiosa en la realización de encuestas", *La Ley Privacidad*, núm. 5, 2020, pág. 4

[22] Un caso similar fue enjuiciado también por la AN, en la sentencia de 22 de febrero de 2019, por recurso interpuesto, en este caso, por la Asamblea Nacional Catalana contra una Resolución de la AEPD que les sancionaba por vulneración los arts. 7.2 y 9 de la LOPD. En este pronunciamiento se disponía textualmente que "*Por todo ello y sin necesidad de valorar si nuestra LOPD, al exigir consentimiento expreso y por escrito en estos casos se ajusta o no a la Directiva europea (que exige consentimiento explícito), lo cierto es que ha quedado probado el tratamiento de datos personales de ideología por parte de la ANC, datos sensibles o*

realización se encargó a una empresa privada externa[23].

5. CONSIDERACIONES FINALES

Como hemos podido constatar en el análisis realizado, el acceso y tratamiento de la información por parte de los partidos políticos supone un grave riesgo, pudiendo implicar una clara vulneración de los derechos de los ciudadanos, y suponiendo un evidente peligro para la salud de la democracia de los países. Dar el poder a los partidos de segmentar a la sociedad, amoldar los mensajes y perfilar a los ciudadanos, para poder dar *publicidad* de sus políticas, promesas electorales, etc., les permite falsear su ideario, y rompe con el debido funcionamiento del sistema democrático.

La normativa europea y la española, en transposición de la anterior, hicieron posible la flexibilización de la tutela de los datos personales en este contexto, algo que encontramos francamente sorprendente y criticable. El RGPD articula una protección estricta y muy desarrollada, con respecto al marco anterior, por lo que no se comprende el porqué de esta desprotección en el ámbito que nos ocupa.

La argumentación desgranada hasta aquí nos lleva a una conclusión clara: desde la perspectiva de la técnica legislativa, la norma es insuficiente y muestra una redacción imprecisa y confusa, en la que, además, están ausentes elementos indispensables (para justificar) la limitación de un derecho fundamental, como es el aquí concernido, en concreto, (la presencia de) las "garantías adecuadas", mentadas en el propio precepto, pero a las que no se vuelve a referir en ningún momento. El problema aquí, en nuestra opinión, es que, dada la naturaleza jurídica del derecho en cuestión, esta regulación sólo puede acometerse mediante una norma del rango adecuado en la jerarquía de fuentes, esto es, mediante otra ley orgánica, en aplicación del principio de reserva de ley consagrado en el art. 53.1 de la

especialmente cualificados que en cualquier caso requieren un reforzamiento de la prestación del consentimiento de su titular para ser objeto de tratamiento.
En definitiva, la ANC trató los datos personales de ideología de los encuestados, sin el consentimiento reforzado que dicho tratamiento de tal categoría especial de datos personales requiere, con vulneración de lo preceptuado en el artículo 7 de la LOPD"

[23] Como resume SEMPERE SAMANIEGO, en este caso "*El Ayuntamiento de Valencia había encargado a una empresa la realización de un estudio sociológico, a través de 1.100 encuestas a falleros e integrantes de comisiones falleras, de forma que desde la óptica de protección de datos, el primero actuaría como responsable y el segundo como encargado de tratamiento. Ambos, habían firmado un contrato en los términos previstos en el artículo 12 de la LOPD, al cual aludiremos más adelante.*
Entre las preguntas controvertidas de la encuesta figuraban las relativas a cuestiones de identidad territorial («si uno se sentía más español que valenciano o viceversa»), condición religiosa («católico, de otra religión o no creyente)», «con qué partido político se siente más identificado», así como una valoración de la orientación política de los encuestados usando una escala del 1 al 10, siendo 1 la extrema izquierda y 10 la extrema derecha." (SEMPERE SAMANIEGO, J., op. cit., pág. 2.)

Constitución Española. Este es, además, el criterio reiterado por la doctrina del Tribunal Constitucional, que ha sostenido en diversos pronunciamientos (STC 290/2000, Fundamentos Jurídicos Décimo primero y Décimo quinto, y la STC 17/2013, Fundamento Jurídico Octavo) que "*existe reserva de ley para fijar las garantías adecuadas y específicas en aquellas disposiciones que sean restrictivas de derechos fundamentales*".

En resumen, debemos ser conscientes de que la regulación que se pretendía introducir, objeto de este análisis, habilitaría una posible clasificación de los ciudadanos, su segmentación por grupos, ideologías y posicionamientos políticos, basándose en información y opiniones plasmadas en foros y redes sociales, emitidos en el marco del ejercicio de sus libertades individuales, protegidas, con un blindaje especial, por nuestra Carta Magna y la Carta Europea de Derechos Fundamentales.[24] Admitir esta posibilidad implicaría abrir la puerta a futuras concesiones a los partidos políticos los cuales, a la vista de los antecedentes conocidos, como el mencionado caso de *Cambridge Analytica*, no conocen límites en su búsqueda de captación de información de los ciudadanos para satisfacer sus intereses, aunque ello atente contra la esfera de derechos de las personas.

Por último, ha quedado evidenciado que las posibilidades que ofrece el estado de la técnica actual en el desarrollo de herramientas digitales agravan el problema, por cuanto permiten una mayor perfección en la captación de la información, incluidos los datos sensibles, su combinación, y tratamiento detallado, haciendo posible la creación de perfiles muy detallados de los usuarios. El avance las técnicas como el Big Data y la IA, y la existencia de lagunas legales o tutelas, en algunos casos, deficientes, de los ciudadanos, presentes en el marco normativo actual, dejan desprotegidos a los titulares. En ese sentido, hemos constata que nuestro Ordenamiento jurídico habilita el uso del "targeting" ("segmentación por categorías genéricas"), lo que permite conocer las opiniones políticas, no así "*microtargeting*" ("perfilado personalizado"). No obstante, las posibilidades que ofrece el Big Data, y la capacidad de las IA para aprender de esa información y tomar decisiones en base a ella, a través un "*machine learning*" cada vez más perfeccionado, facilitan la realización de actividades y conductas enfocadas, con un alto nivel de personalización, a

[24] Opinión sostenida, asimismo, por SANZ, considerando que "*si se permitiese que los partidos pudiesen hacer grupos de ciudadanos clasificados por sus ideas políticas, y estos grupos los formasen los propios partidos por la participación de los ciudadanos en las redes sociales, no se puede saber qué podría ser lo siguiente. Lo mismo la profecía de Orwell se quedaba corta*." (SANZ PÉREZ, A. L., "La protección de datos personales y los partidos políticos", *Revista Aranzadi Doctrinal*, núm.8/2019 parte Jurisprudencia. Doctrina, Ed. Aranzadi, 2019; págs. 2 y 7.)

los sujetos, sin necesidad de una individualización previa de éstos.

REFERÊNCIAS

ADSUARA VARELA, B., “El «perfilado ideológico» de los ciudadanos por los partidos políticos”, *El Consultor de los Ayuntamientos*, Núm. III, Sección Crónica, Julio 2019.

ADSUARA, B. y MARTINEZ, R., “Debate sobre el nuevo artículo 58 bis de la LOREG”, LA LEY privacidad, Núm. 1, Wolters Kluwer, 2019.

ALLCOTT, H. y GENTZKOW, M., “Social Media and Fake News in the 2016 Election (Spring 2017)”, Stanford University, *Journal of Economic Perspectives*, Vol. 31, No. 2, 2017.

ALTHEUNER, F. y BIETTI, E., “Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR”, *Journal of Information Rights, Policy and Practice*, 2(2), 2018.

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,* Editorial Wolters Kluwer, 2018.

KALTHEUNER, F., BIETTI, E., “Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR”, J*ournal of Information Rights, Policy and Practice* (IRP&P), Winchester University Press, 2018.

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

SANTOS SANCHEZ, D. J., “Comentario del Informe 2018-0181 y la Circular 1/2019 de la AEPD, sobre tratamiento de datos relativos a opiniones políticas por partidos políticos”, La Ley Privacidad, núm. 1, 2019.

SANZ PÉREZ, A. L., “La protección de datos personales y los partidos políticos”, *Revista Aranzadi Doctrinal*, núm.8/2019 parte Jurisprudencia. Doctrina, Ed. Aranzadi, 2019.

SEMPERE SAMANIEGO, J., “Tratamiento de datos de ideología política y religiosa en la realización de encuestas”, *La Ley Privacidad*, núm. 5, 2020.

ZUIDERVEEN BORGESIUS, F. & TRILLING, D. & MÖLLER, J. & BODÓ, B. & DE VREESE, C. & HELBERGER, N., “Should we worry about filter bubbles?”, *Internet Policy Review*, núm. 5(1).

Recebido em 15/04/2023.
Aprovado em 28/04/2023.
Received in 15/04/2023.
Approved in 28/04/2023.