LA INCONSTITUCIONAL HABILITACIÓN A LOS PARTIDOS POLÍTICOS PARA RECABAR DATOS SOBRE OPINIONES POLÍTICAS. COMENTARIO A LA STC 76/2019, DE 22 DE MAYO

The unconstitutional enabling of political parties to collect data about political opinions

DANIEL JOVE VILLARES
Universidad de La Coruña
d.jove.villares@udc.es

Cómo citar/Citation
Jove Villares, D. (2021).
La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de mayo.
Revista Española de Derecho Constitucional, 121, 303-331.
doi: https://doi.org/10.18042/cepc/redc.121.10

Resumen

El día 22 de mayo de 2019, el pleno del Tribunal Constitucional declaró la inconstitucionalidad del apdo. 1 del art. 58 *bis*. Este precepto, incorporado a la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, fue recurrido ante el Alto Tribunal español por el Defensor del Pueblo. La inconstitucionalidad del precepto se fundamenta en una triple vulneración del derecho a la protección de datos en conexión con el art. 53.1 de la Constitución: la ausencia de una finalidad definida que justifique la injerencia en el derecho, la inexistencia de límites claros y la no regulación de un adecuado marco de garantías.

Palabras clave

Protección de datos; partidos políticos; opiniones políticas; datos especiales; RGPD; LOPDGDD; Tribunal Constitucional.

Abstract

On 22 May 2019, the Constitutional Court declared unconstitutional Article 58 bis (1). This provision, incorporated into Organic Law 5/1985, of 19, June on the General Electoral System by Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights was appealed by the Ombudsman. The unconstitutionality of article 58 bis is based on a triple violation of the right to data protection in connection with article 53.1 of the Constitution: the absence of a defined purpose that justifies interference in the right to data protection, the lack of clear limits and the legislator's failure to regulate an adequate framework of guarantees.

Keywords

Data protection; political parties; political opinions; special categories of personal data; GDPR; LOPDGDD; Constitutional Court.

SUMARIO

I. LA DEMOCRACIA EN LA ERA DIGITAL. UN ADELANTO DE LOS PROBLEMAS QUE ESTÁN POR VENIR

El aforismo «el conocimiento es poder» alcanza nuevas dimensiones en la era digital. La cantidad de datos que hoy pueden recabarse, tratarse e interrelacionarse es abrumadora. La agregación y el cruce de datos facilitados por el *big data* y la inteligencia artificial proporcionan nuevas informaciones, distintas de los datos originarios. Las inferencias y predicciones resultantes pueden alcanzar un elevado nivel de fiabilidad y certeza, hasta el punto de hacernos olvidar su naturaleza conjetural y probabilística[1].

La consolidación de tecnologías basadas en el tratamiento masivo de datos y la solución algorítmica a problemas y decisiones de la vida diaria (algunas tan triviales como dónde comer y otras tan relevantes como determinar si una persona puede recibir un préstamo, contratar un seguro o recibir atención sanitaria privada) afectan al modo en que la sociedad se organiza y

[1] El nivel de precisión tiene, como variables más destacadas, la cantidad y la calidad de los datos. No obstante, habrá informaciones que no se conozcan, o sean imposibles de incorporar a los sistemas algorítmicos, y cuya transcendencia puede afectar a la fiabilidad del resultado final. Un ejemplo del carácter predictivo, no siempre acertado, de estos sistemas puede verse en Lazer *et al.* (2014).

desarrolla. «La capacidad humana para decidir libremente está colapsando» (Lassalle, 2019: 30) o, al menos, viéndose severamente amenazada. Queda, así, expedito el paso para el surgimiento de un «Leviatán tecnológico […] desde el que se reorganizará la arquitectura artificial de un poder concebido como un panóptico perfecto» (*ibid*.: 48).

La formación de la voluntad política, la competencia partidista por atraer y convencer al electorado acerca de las posiciones propias o, cuanto menos, la articulación de una estrategia que los aleje de las contrarias, también es objeto de las nuevas posibilidades surgidas con la era digital. Los análisis sobre las tendencias del voto procesan multitud de datos que permiten cuantificar y estratificar (por edades, por sexo o por preferencias) a los votantes y anticipar sus preocupaciones e intereses. Estos estudios aportan elementos especialmente anhelados en la arena política, cruciales para el diseño de la estrategia electoral. Las encuestas, los grupos de control, el conocimiento del censo electoral o los resultados de las diferentes mesas son datos de gran valor para los partidos y las organizaciones políticas.

La tecnología ha ampliado el abanico de posibilidades y modos de conectar con el electorado y, sobre todo, de incidir en la conformación de su voluntad. Buena muestra de este nuevo escenario son el uso de técnicas como el *microtargeting*, adoptando, incluso, «técnicas militares de ataque psicológico» (Suárez-Gonzalo, 2018: 27), o la elaboración de noticias poco veraces, cuando no directamente falsas, destinadas a sectores específicos de población.

El *big data*, los algoritmos, la inteligencia artificial y el envío selectivo de noticias falsas creadas por *bots* desempeñan —y desempeñarán— un papel estratégico en la lucha por el poder —también político—. Todavía es aventurado precisar el nivel de influencia exacta que la utilización de estas técnicas puede tener en la conformación de la decisión final del voto, pero, sin mucho temor a errar la predicción, es más que probable que, conforme mejoren esas técnicas, su grado de incidencia aumente exponencialmente. Los datos personales —y los anonimizados— son, al tiempo, mecha y combustible de todas las técnicas mencionadas y, seguramente, de las que se creen en los próximos años.

El panorama descrito refleja la confluencia de dos peligros diferentes que convergen en el ámbito de los datos personales. De una parte, las posibles vulneraciones del derecho fundamental que garantiza su protección. De otra, los peligros que, para la pervivencia del sistema democrático, puedan derivarse de determinados usos de las tecnologías de la información.

Esta última es una amenaza de contornos difusos, cuyo peligro real resulta difícil de cuantificar, porque ¿cuánto influyen en la decisión final?, ¿cuánto la condicionan?, ¿cuánto hacen variar el resultado respecto al que se

obtendría si estas no existieran? La respuesta a estas preguntas es incierta, pero el riesgo que las justifica es muy real. La mera sospecha —no digamos la confirmación— acerca del uso de técnicas tendentes a falsear o alterar el resultado de unas elecciones provoca un efecto de desaliento (*chilling efect*) tanto sobre la libertad de voto como acerca de la confianza en el sistema establecido, que, en última instancia, provocaría «el debilitamiento de la propia esencia de la democracia» (Arenas Ramiro, 2019: 370).

Las amenazas y peligros aquí apuntados se han visto materializados en asuntos tan conocidos como el de *Cambridge Analytica*[2], ejemplo paradigmático de las potencialidades del tratamiento masivo de datos. El riesgo de ver jaqueados los procesos electorales es una realidad contrastable y no un mero ejercicio probabilístico, ya sea por actuaciones de sus protagonistas —valiéndose de las posibilidades que la tecnología les ofrece para influir/condicionar la decisión del ciudadano a niveles nunca antes conocidos—, ya por la injerencia de agentes externos con intereses de lo más diversos[3].

Ante este horizonte corchado de nubarrones, resulta crucial la adopción de nuevas medidas que aseguren la libre formación de la voluntad personal y protejan los derechos y libertades de la ciudadanía. En este contexto, la protección de datos desempeña un rol central, al establecer el modo y las condiciones en las que ha de operarse con el sustrato que alimenta este tipo de tecnologías. A pesar de ello, sería un error considerar que la simple adopción de prácticas respetuosas con este derecho es una suerte de panacea capaz de conjurar todos los peligros derivados del uso de esta tecnología.

Hay otros derechos y actuaciones que pueden contribuir a minimizar los efectos perturbadores del mal uso de los instrumentos digitales, *v. gr.*, una mayor transparencia, apostar por modelos que aseguren el acceso a información veraz y que, a la vez, contrarresten, o al menos debiliten, los efectos de las *fake news*; pero, sobre todo, fomentar la formación digital[4] de la ciudadanía, no solo desde el punto de vista técnico, sino, también, en valores y derechos. Es necesario generar un espíritu crítico que permita salir a flote del caudaloso torrente de información existente.

---

2 Sobre cómo operaba Cambridge Analytica, véase Villalobos Guízar (2018).

3 Sobre el papel que desarrolla la tecnología a la hora de interferir en los procesos electorales de otros países, véase Torres Soriano (2017).

4 La LOPDGDD incorpora, en el art. 83 el derecho a la educación digital; sin duda es una medida oportuna y pertinente, aunque necesita de una apuesta política decidida para lograr todo su potencial.

Descrito de forma muy sucinta, este es el contexto de referencia[5] en el que debe encuadrarse el art. 58 *bis* de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido mediante la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).

II. EL CONTEXTO DE LA SENTENCIA: LA DISPOSICIÓN FINAL 3.ª DE LA LOPDGDD, LA AEPD Y EL DEFENSOR DEL PUEBLO

1. EL ORIGEN DEL CONFLICTO. LA DISPOSICIÓN FINAL 3.ª DE LA LOPDGDD

Los partidos políticos, las asociaciones, las federaciones o las agrupaciones electorales que median en los procesos de participación política necesitan tratar información personal para desarrollar su actividad diaria. Datos de todo tipo, desde los más instrumentales, como pueden ser los necesarios para la gestión de sus empleados (*v. gr.*, nóminas), hasta los contenidos en el censo electoral[6], pasando por otro tipo de informaciones, imprescindibles para ordenar el funcionamiento ordinario de la organización, como son las relativas a proveedores o militantes. Ahora bien, entre los datos que tratan, no todos poseen la misma enjundia, ni se les aplica el mismo régimen de protección. No todos tienen la misma capacidad de afectación de los derechos fundamentales.

---

5 En este sentido se pronuncia la motivación de la enmienda 331, de la que el art. 58 *bis* trae causa. De hecho, menciona expresamente el caso *Cambridge Analytica* como ejemplo de situación que impedir. Véase *BOCG*, Congreso de los Diputados, XII legislatura, 18 de abril de 2018, n.º 13-2, Serie A, p. 209.

6 Si bien es cierto que el tratamiento de los datos del censo está restringido al período de campaña electoral, salvo consentimiento expreso del interesado, como recuerda García Mahamut (2015: 319). Por otra parte, debe apuntarse que los tratamientos que tengan por objeto los datos obrantes en el censo se regirán por las disposiciones específicas de la LOREG. Véanse el art. 2.3 LOPDGDD y los arts. 31, 32 y 41 de la LOREG. Aunque emitido antes de la promulgación del RGPD, el informe 0244/2014 de la AEPD resulta muy clarificador respecto del régimen jurídico que rige el tratamiento de los datos obrantes en el censo electoral, así como sobre las excepcionales circunstancias en que resulta posible el ejercicio del derecho de oposición por los electores frente a dicho tratamiento. Puede consultarse el informe en https://bit.ly/3aOEuJ6 (última consulta: 14-12-2020).

El ejemplo más paradigmático es el registro de los afiliados, que contiene una información especialmente sensible por cuanto revela la orientación ideológica de quienes figuran en él. Este registro es muy anterior a la era digital, ahora bien, la emergencia de esta y la consiguiente automatización del tratamiento de los datos personales han supuesto un aumento de los riesgos para los derechos fundamentales (Troncoso Reigada, 2010: 32), debido a la mayor inmediatez y capacidad de procesamiento de información que la tecnología posibilita.

Para afrontar los peligros que el tratamiento automatizado de la información genera ha de atenderse a la naturaleza de los datos con los que se opera. En nuestro ordenamiento jurídico, las «opiniones políticas» son incluidas en una de las categorías de datos especiales[7], es decir, tipologías de «datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales»[8]. Esa potencial capacidad de afectación e incidencia sobre los derechos fundamentales es la que, en última instancia, justifica que los datos especiales tengan un régimen de protección específico y mucho más reforzado (Zarsky, 2017: 1012), al punto de ser la prohibición de su tratamiento la regla, admitiéndose su excepción solo cuando concurra alguna de las circunstancias previstas en el apdo. 2 del art. 9 del 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) (en adelante, RGPD). Esta norma europea remite, en no pocas ocasiones, «al derecho nacional para determinar el alcance último de los límites y posibilidades de los tratamientos, […] [constatándose, así,] que el RGPD tiene alma de Directiva, habida cuenta de la libertad que confiere a los Estados para culminar la regulación de determinados aspectos» (Medina Guerrero, 2019: 256).

---

7 Conforme a lo establecido en el art. 9.1 del 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) (en adelante, RGPD), serán datos especiales aquellos «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 sexuales de una persona física».

8 Considerando 51 RGPD.

Retomando el ejemplo del registro de los afiliados, los partidos pueden tratar esas informaciones —cuando cuenten con la imprescindible base de legitimación para ello[9]— siempre que se circunscriban al «ámbito de sus actividades legítimas y con las debidas garantías […] [y] que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos»[10]. Es decir, solo cuando se produzca alguna circunstancia que enerve la prohibición de tratar datos referidos a opiniones políticas, los partidos podrán gestionar este tipo de información.

El tratamiento de datos especiales demanda unas cautelas adicionales, además de estar jurídicamente acotado a supuestos muy concretos. De hecho, en la relación de circunstancias que habilitan el tratamiento de datos especiales se incluyen, expresamente, aquellas en las que «el tratamiento es necesario por razones de un interés público esencial»[11]. Esta fue la percha utilizada por el legislador español para permitir a los partidos políticos «la recopilación de datos personales relativos a las opiniones políticas de las personas»[12].

Junto con la apuntada recopilación de datos personales (cuestión a la que se prestará especial atención por ser el objeto de la sentencia comentada), la disposición final tercera de la LOPDGDD[13] regula, mediante la incorporación del art. 58 *bis* a la LOREG[14], toda una serie de supuestos relativos al tratamiento y uso de información por parte de los partidos políticos, coali-

---

9 Las bases de legitimación están tasadas y son las previstas en el art. 6 del RGPD.

10 Art. 9.2.d) del RGPD.

11 Art. 9.2.g) del RGPD.

12 Art. 58 *bis*, apdo. 1, LOREG.

13 Puede consultarse un análisis detallado de las implicaciones y consecuencias jurídicas de este precepto en García Herrero (2019: 295-321).

14 Art. 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 período 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.

ciones y agrupaciones electorales. En su apdo. 2 posibilita que los partidos y demás entidades mencionadas puedan utilizar datos personales —en general, no solo los referidos a opiniones políticas— siempre que consten en «páginas web y otras fuentes de acceso público», es decir, aquellos que cumplan con el principio de transparencia y que sean datos hechos manifiestamente públicos por el interesado. Empero, se instituyen dos límites: a) el tratamiento ha de tener como finalidad «la realización de actividades políticas» y b) solamente se podrá realizar «durante el período electoral».

Abundando en la misma dirección regulatoria, el apdo. tercero del art. 58 *bis* establece un régimen particularizado para la propaganda electoral. La excluye de los supuestos sometidos a la regulación relativa a las comunicaciones comerciales[15], tanto en lo referente a su «envío […] por medios electrónicos» como en lo que respecta a su «contratación […] en redes sociales o medios equivalentes».

Finalmente, los apdos. cuarto y quinto imponen a los actores electorales dos obligaciones: informar «de modo destacado» sobre la naturaleza electoral de los envíos y actuaciones de propaganda (apdo. 4), y facilitar el ejercicio del derecho de oposición por los ciudadanos «de un modo sencillo y gratuito» (apdo. 5). Ante la falta de mayor precisión normativa, cabe entender que el ejercicio del derecho de oposición procederá no solo frente a los envíos de propaganda electoral, sino, también, ante el tratamiento de datos del apdo. 2 del art. 58 *bis*[16].

Por su parte, el apdo. primero del art. 58 *bis* —el apartado sobre cuya constitucionalidad se pronuncia TC— invoca la existencia de un interés público que, sin embargo, no identifica. La remisión a ese interés público necesitado de salvaguarda conecta el tratamiento de datos previsto en ese apdo. primero con la circunstancia habilitante para el tratamiento de datos especiales del 9.2.g) del RGPD[17]. No obstante, en este último precepto se exige un interés público

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

15 Por lo tanto, no le será de aplicación el art. 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Este precepto prohíbe los envíos publicitarios, salvo que medie solicitud, autorización expresa o relación contractual previa.

16 No se ha incluido el tratamiento de datos regulado en el apdo. 1 del art. 58 *bis* como susceptible de serle aplicable el derecho de oposición por haber sido declarado inconstitucional en la sentencia objeto de comentario.

17 Art. 9.2.g) RGPD: «[…] 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

«esencial», lo que indica que el parámetro es más exigente y demanda de una mayor concreción. Por si no fuese razón suficiente, la legislación española establece que el tratamiento ha de derivar «de una competencia atribuida por una norma con rango de ley» (art. 8.2 LOPDGDD), con las garantías que ello requiere en cuanto a configuración y contenido. En definitiva, es imperativo para el legislador precisar qué interés público «esencial» justifica la injerencia en el derecho a la protección de datos. No basta una razón general.

Ahora bien, el legislador español no solo se apoyaba en lo dispuesto en el art. 9.2 del RGPD al reconocer esa atribución a los partidos políticos. También estaba acogiéndose a la habilitación que el RGPD hace a los legisladores nacionales en el considerando 56[18]. Este abre la puerta —que no obliga a traspasar— para que los partidos políticos, «en el marco de actividades electorales» y cuando «el funcionamiento del sistema democrático» lo exija, puedan recopilar «datos personales sobre las opiniones políticas de las personas». El legislador español tampoco se ha molestado de identificar, aunque fuese de forma orientativa y genérica, qué se entiende por «funcionamiento del sistema democrático» a los efectos de estimar que los partidos políticos puedan recabar las opiniones políticas de los ciudadanos.

El legislador español no es el único que ha regulado esta cuestión. En el Reino Unido —donde está acreditado que Cambridge Analytica realizó actuaciones tendentes a influir en el resultado final del *brexit*[19]— la *Data Protection Act 2018* permite a los partidos políticos operar con datos que revelen opiniones políticas, siempre que sea necesario para el ejercicio de sus actividades[20]. No obstante, las posibilidades de actuación de los partidos ingleses no son incondicionadas. Así, no podrán llevar a efecto tratamientos que puedan causar daño a una persona o que le afecten de tal modo que le generen una angustia sustancial (*substantial distress*)[21], ni tampoco cuando el

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».

18 Considerando 56 del RGPD: «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».

19 Pueden consultarse los documentos que vinculan a Cambridge Analytica y Leave. EU en: https://bit.ly/3cW4aWW (última consulta: 14-12-2020).

20 *Data Protection Act 2018, Schedule 1, part 2, political parties*, art. 22.1.c).

21 *Data Protection Act 2018, Schedule 1, part 2, political parties*, art. 22.2: «Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to a person».

interesado se haya opuesto, mediante una notificación por escrito, a que se traten sus datos[22].

El elemento diferenciador da la regulación británica es que —a diferencia del apdo. uno del art. 58 *bis*— sí establece una definición de lo que son actividades políticas, entre las que incluye: campañas, recaudación de fondos, encuestas políticas y el trabajo de casos[23]. El grado de concreción importa cuando se regulan las posibilidades de tratamiento de información personal.

2. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y SU INTENTO DE ENDEREZAR Y CLARIFICAR EL PRECEPTO

El precepto objeto de estudio, singularmente su apdo. primero, dio lugar a una importante polémica y fue motivo de preocupación, incluso, antes de su aprobación definitiva en el Senado. En los días previos, especialistas en privacidad[24] y medios de comunicación advirtieron sobre los riesgos que, para la privacidad, implicaba la disposición final tercera. Sobre todo, apercibieron de los peligros que podía suponer consentir que las organizaciones políticas pudiesen llegar a elaborar perfiles de los ciudadanos, de sus orientaciones y preferencias políticas y electorales. Especialmente, cuando dicha posibilidad se fundaba en una previsión con un elevado grado de indeterminación.

La Agencia Española de Protección de Datos (en adelante, AEPD) publicó, el mismo día en que se votaba la LOPDGDD[25], una nota informativa en la que señalaba cuáles serían sus criterios a la hora de afrontar la resolución de cuestiones electorales[26]. Pese al pronunciamiento de la AEPD, y al informe —más pormenorizado— publicado días después[27], las dudas sobre la

---

22 *Data Protection Act 2018, Schedule 1, part 2, political parties*, art. 22.3.

23 *Data Protection Act 2018, Schedule 1, part 2, political parties*, art. 22.4: «Political activities include campaigning, fund-raising, political surveys and case-work».

24 Deben destacarse las advertencias realizadas por Jorge García Herrero o Borja Adsuara. Pueden consultarse sus publicaciones durante los días previos y posteriores a la aprobación de la LOPDGDD en: https://bit.ly/37dt54H y https://bit.ly/3q80rsY, respectivamente (última consulta: 27-11-2019).

25 Quedando aprobada en el Senado con 221 votos a favor y 21 en contra de UP, Compromís, Nueva Canarias y Bildu, rompiéndose, así, la unanimidad que hasta el momento había presidido la tramitación de la LOPDGDD. El factor principal que justifica esos votos contrarios a la LOPDGDD fue, precisamente, la disposición final tercera de la LOPDGDD.

26 Disponible en: https://bit.ly/2Z2Ie40 (última consulta: 14-12-2020).

27 Puede consultarse en: https://bit.ly/2LE7vyE (última consulta: 14-12-2020).

constitucionalidad del precepto persistieron. Entre otras razones porque la interpretación de la AEPD era solo una de las posibles y nada garantizaba que ese criterio se fuese a sostener en el tiempo.

Para tratar de despejar las inseguridades jurídicas del precepto[28] —especialmente sus lagunas— y paliar, interpretativamente, los riesgos y carencias del art. 58 *bis*, especialmente de su apdo. primero, la AEPD publicó la 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 art. 58 *bis* de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

La AEPD no trataba de realizar algo que, como es obvio, le está vedado —solventar la constitucionalidad de la ley—, sino que buscaba ofrecer seguridad y garantías en su aplicación. Para ello estableció los criterios que iba a seguir en sus actuaciones, de manera tal que los tratamientos de los partidos políticos que no se acomodasen a lo dispuesto en la circular serían objeto de fiscalización por la AEPD. No podía resolver el entuerto generado por el legislador en el art. 58 *bis*, pero sí paliar sus efectos.

En aras de lograr este objetivo, la circular define qué ha de entenderse por «actividades electorales», acotándolas a las llevadas a cabo «durante el período electoral y respecto de las actividades de propaganda y actos de campaña electoral» (art. 4.1 de la circular). Por lo tanto, considera que ambos momentos son coincidentes en cuanto a su extensión[29], de suerte que solo dentro de ese marco temporal pueden los partidos políticos efectuar este tipo de tratamientos. Además, precisa que los partidos políticos solo podrán recabar aquellas opiniones políticas que hubiesen sido «libremente expresadas» (art. 5.1 de la circular) y obtenidas de fuentes de acceso público[30] (art. 5.3 de la circular).

A estas matizaciones ha de adicionarse la incorporación de un completo catálogo de garantías (art. 7 de la circular) y un conjunto de indicaciones acerca de cómo y cuándo procede adoptar cada una de las medidas dirigidas

[28] En la exposición de motivos de la Circular 1/2019 se reconoce que el legislador no ha establecido garantías frente al «alto riesgo para los derechos y libertades de las personas físicas» que suponen los tratamientos de datos habilitados.

[29] Véase la sección IV de la LOREG, relativa a las disposiciones generales sobre la campaña electoral.

[30] Entendidas como «aquellas cuya consulta puede ser realizada por cualquier persona» (art. 5.3 de la circular).

a asegurar un tratamiento de datos personales respetuoso con los derechos y libertades constitucionales (art. 9 de la circular). La disposición comentada también refuerza las exigencias de información (art. 8 de la circular) y excluye la opción de tratar «otro tipo de datos personales» cuando el objetivo último del tratamiento sea «inferir[31] la ideología política de una persona» (art. 5.2 de la circular).

Al descartar la posibilidad de colegir, a través de técnicas de tratamiento masivo de datos e inteligencia artificial, la tendencia ideológica de una persona, el propósito de la AEPD es meridiano: cortar de raíz uno de los peligros más relevantes del *big data* aplicado a los escenarios políticos y electorales: la distorsión del ejercicio del derecho al voto, al alterar la libre formación de la voluntad. La misma razón explica, también, la prohibición del *microtargeting* (art. 6 de la circular). La AEPD actuó con celeridad, valiéndose de los instrumentos jurídicos a su alcance para tratar de ofrecer seguridad, mediante la concreción de lo dispuesto en el art. 58 *bis*. Con su circular descartaba eventuales interpretaciones que pudiesen suponer una amenaza cierta para el normal discurrir de los procesos electorales[32].

Por muy oportunas que pudieran ser las medidas adoptadas, por reseñables que sean las salvaguardas que la circular establece, ello no cambia su naturaleza infralegal. Ni la circular, ni ninguna disposición de la AEPD pueden, como es obvio, sanar los vicios de inconstitucionalidad de una ley. Con todo, no puede negarse que es un complemento útil. En la actualidad, y declarada la inconstitucionalidad del apdo. primero del art. 58 *bis*, sigue siendo aplicable a los demás apartados de ese precepto. Especialmente apropiadas son las indicaciones que realiza respecto de la ejecución de la comunicación de propaganda electoral por medios electrónicos.

3. EL APARTADO PRIMERO DEL 58 *BIS* LLEGA AL TRIBUNAL CONSTITUCIONAL

Las dudas surgidas en torno a la constitucionalidad de la disposición final tercera (mediante la que se añade el art. 58 *bis* a la LOREG) hicieron que los consensos y la sintonía, que hasta entonces habían presido la elaboración y

[31] Sobre la naturaleza jurídica de las informaciones obtenidas mediante inferencias, véase Wachter y Mittelstadt (2019).

[32] La mención específica de estas prácticas no es casual, sino que se trata de los mecanismos de los que se valió Cambridge Analytica para tratar de influir en los diferentes procesos electorales en que prestó sus servicios. Véase Villalobos Guízar (2018).

tramitación de la LOPDGDD, se quebrasen. Recordemos que varios senadores, conscientes del aumento de las voces críticas sobre el contenido del precepto, votaron, finalmente, en contra de su aprobación.

No obstante, no fueron ni diputados ni senadores quienes, al amparo de la legitimación que constitucionalmente se les confiere (art. 162.1.a CE), impugnaron el precepto ante el Tribunal Constitucional[33], sino el Defensor del Pueblo[34]. Tomando en consideración la naturaleza del problema y las solicitudes ante él presentadas, interpuso un recurso de inconstitucionalidad contra el apdo. primero del art. 58 *bis*[35]. Si bien es cierto que, en los escritos que se le remitieron se incluían otros apartados del precepto (p. ej., 2 y 3), en los que los solicitantes apreciaban carencias y problemas equiparables a los del apdo. primero[36].

El recurso de inconstitucionalidad fue resuelto con una inusual celeridad[37], como si el Tribunal Constitucional se dejase llevar por los dictados de la era de la inmediatez en la que estamos inmersos y tan relacionada con el objeto del asunto. El 22 de mayo de 2019, apenas tres meses después de haberse registrado el recurso, el pleno, por unanimidad, despejó las dudas jurídicas que se habían suscitado sobre la constitucionalidad del apdo. 1 del art. 58 *bis*.

4. UN PRECEPTO Y MUCHOS INTERROGANTES

El art. 58 *bis* había generado diversos interrogantes jurídicos. Desde la posible afectación de la libertad ideológica y el derecho de participación hasta la insuficiente justificación de su base de legitimación, pasando por la ausencia de garantías y la consiguiente vulneración del derecho *ex* art. 18.4 CE.

---

33 UP, que había votado en contra en el Senado, y contaba con suficientes diputados para presentar el recurso, no llegó a presentarlo.

34 El recurso presentado por el Defensor del Pueblo, disponible en: https://bit.ly/3a-2bLRN (última consulta: 14-12-2020).

35 Sobre los antecedentes y la presentación de la petición al Defensor del Pueblo, así como las líneas básicas de la sentencia, véase Adsuara Varela (2019).

36 El escrito de la solicitud de recurso al Defensor del Pueblo, así como quienes lo impulsaron, está disponible en: https://bit.ly/2MGEkeS (última consulta: 14-12-2020).

37 El recurso fue resuelto en menos de tres meses, desde que el Defensor del Pueblo lo presenta en marzo hasta el 22 de mayo, fecha de la Sentencia 76/2019, con la que se resuelve.

Para el Tribunal Constitucional, que, en este punto, asumió la tesis del demandante[38], el nudo gordiano consistía en determinar si el transcrito apdo. 1 del art. 58 *bis* reunía los requisitos y garantías imprescindibles para justificar —y hacer constitucionalmente asumible— esa injerencia en el derecho fundamental a la protección de datos. O si, por el contrario, dicho precepto vulneraba su contenido constitucionalmente protegido, incluida la reserva de ley del 53.1 CE.

La transcendencia de este motivo de impugnación se evidencia en el hecho de que, una vez constatada la inconstitucionalidad del precepto por esta causa, el TC consideró innecesario analizar el resto de los argumentos alegados por el Defensor del Pueblo[39]. Ahora bien, a pesar de que no tuvieron acogida expresa en la sentencia, no por ello dejan de ser estimables y útiles como objeto de reflexión, singularmente en lo que atañe a la hipotética conculcación de la libertad ideológica (art. 16 CE) y del derecho de participación política (art. 23 CE)[40].

La eventual vulneración de estos dos derechos fundamentales derivaría de la naturaleza de los datos tratados. El tratamiento de informaciones relativas a las tendencias ideológicas de los ciudadanos, con vulneración del derecho a la protección de datos, pone de manifiesto uno de sus elementos definitorios: su carácter instrumental (Troncoso Reigada, 2010: 73). Esta instrumentalidad se manifiesta, de manera más elocuente[41], cuando —como es el caso— los datos objeto de tratamiento son especiales. Estaríamos ante tratamientos en los que el derecho a la protección de datos no solo asegura al ciudadano un «poder de disposición y de control»[42], sino que, además, actúa como garantía y protección adicional de otros derechos fundamentales que

---

38 La Abogacía del Estado, por su parte, consideraba que la cuestión central que resolver era si existía vulneración del principio de seguridad jurídica (9.3 CE), pues, de garantizarse esta, por prever el precepto las garantías adecuadas, decaerían las demás impugnaciones de la defensoría del pueblo.

39 STC 76/2019, de 22 de mayo, FJ 9.

40 FF. JJ. quinto y sexto del recurso del Defensor del Pueblo.

41 Aunque resulta más claro el carácter instrumental cuando el tratamiento involucra datos especiales, ese valor es pregonable para todo tipo de datos y tratamientos, como certeramente apuntó el TC en la STC 292/2000, de 30 de noviembre, FJ 7: «El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado».

42 STC 292/2000, de 30 de noviembre, FJ 7.

también pueden verse vulnerados (como pueden ser la intimidad o, en este caso, la libertad ideológica y el derecho de participación política).

III. UN PRECEPTO Y TRES VULNERACIONES DE LA CONSTITUCIÓN

El núcleo de la pretensión actora lo constituye la alegada vulneración del 18.4 de la CE en conexión con el 53.1 CE. La respuesta ofrecida por el Tribunal es tan rotunda como inequívoca. El 58 *bis*, en su apdo. 1, incurre en «tres vulneraciones […] autónomas e independientes entre sí, todas ellas vinculadas a la insuficiencia de la ley y que solo el legislador puede remediar»[43]. Pero ¿cuáles son esas vulneraciones?

Según el Tribunal, el precepto no concreta el interés público esencial que se salvaguardaría y que justificaría la injerencia en el derecho fundamental; tampoco «limita el tratamiento regulando pormenorizadamente las restricciones al derecho»[44] y, finalmente, no establece las «garantías adecuadas frente a la recopilación de datos personales»[45].

1. ¿QUÉ INTERÉS PÚBLICO SE PRETENDÍA PROTEGER?

El consentimiento ha sido, desde la LORTAD, la base sobre la que, tradicionalmente, se ha construido el sistema de protección de datos en España[46]. El propio TC, en la conocida STC 292/2000, lo situó en el centro del derecho a la protección de datos[47]. Mientras la Directiva 95/46/CE

43 STC 76/2019, de 22 de mayo, FJ 9.

44 STC 76/2019, de 22 de mayo, FJ 7.

45 STC 76/2019, de 22 de mayo, FJ 8.

46 Arts. 6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

47 STC 292/2000, de 30 de noviembre, FJ 7: «Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos».

«contemplaba seis causas de legitimación, todas con el mismo fundamento y sin prevalencia de unas sobre otras» (Puente Escobar, 2019: 120), en España el consentimiento gozaba de un carácter preferente, teniendo las demás bases de legitimación un carácter más bien complementario[48].

Este modelo de tratamiento cambia radicalmente con la aprobación del RGPD, que configura, de manera indiscutible y para todos los países de la Unión Europea, un sistema de protección con seis bases diferenciadas de legitimación y el mismo nivel de preeminencia. La normativa española va un paso más allá y establece, en el art. 9.1 LOPDGDD, que «el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar […] [la] ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico». La otrora condición privilegiada del consentimiento como base de legitimación es un recuerdo del pasado.

Siendo ello así, no debe sorprender que se pueda aducir como base legal del tratamiento la existencia de un interés público que salvaguardar (art. 6.1.e RGPD). En este sentido, cabe recordar que la LOPDGDD ha incorporado un requisito adicional para apoyarse en esta base de legitimación, al exigir que el tratamiento «derive de una competencia atribuida por una norma con rango de ley» (art. 8.2 LOPDGDD). No obstante, si el tratamiento que se pretende realizar requiere de la utilización de datos especiales, no será suficiente la mera existencia de un genérico interés público, sino que ha de acreditarse que se está en presencia de un «interés público esencial» (9.2.g del RGPD).

El escenario final resulta, por tanto, bastante complejo. En primer lugar, el aplicador de la norma ha de lidiar con el elevado grado de indeterminación del concepto interés público[49]. Y, en segundo lugar, porque, una vez identificado, habrá de acreditar que ese interés público tiene la suficiente entidad como para enervar la prohibición inicial de tratar datos especiales. La concreción de lo que significa «esencial», en cada particular situación, no es tarea fácil de acometer, pues tiene un importante componente subjetivo y discrecional que, probablemente, solo la jurisprudencia podrá aclarar caso por caso.

Lo que sí parece claro es que habrá de tratarse de un interés inequívocamente público y, además, debe revestir una entidad suficiente para justificar que la exclusión de la citada prohibición resulte proporcionada y adecuada. Para García Sanz, las finalidades que avalarían la existencia de un interés público

[48] En el caso del interés legítimo (art. 7.f), ni siquiera se contemplaba en la LOPD de 1999.

[49] Sobre la complejidad de determinar qué ha de entenderse por interés público, véase Salas Carceller (2014).

esencial, en el caso que nos ocupa, son «depurar y formar la opinión pública electoral, para que el derecho de participación despliegue sus efectos en los procesos democráticos y en la campaña electoral» (2019: 157).

Si se analiza el apdo. primero del art. 58 *bis* a la luz de estas exigencias, es fácil apreciar que el legislador no identifica de manera clara y fehaciente el interés público esencial que, en su caso, debería amparar la afectación del derecho a la protección de datos. A lo sumo, realiza una genérica apelación a la salvaguarda del sistema democrático, lo que, en última instancia, poco aporta a la hora de identificar la finalidad específica que justificaría la injerencia en el derecho. Además, la vaguedad de ese estándar normativo tampoco permite valorar la «idoneidad, necesidad y proporcionalidad»[50] de la medida.

En la sentencia objeto de este comentario, el TC mantiene la doctrina establecida en la STC 292/2000 y, en coherencia con ella, niega la posibilidad de restringir el derecho a la protección de datos amparándose en «la identificación de los fines legítimos […] mediante conceptos genéricos o fórmulas vagas» (FJ 7). La carencia de concreción y certidumbre se convierte, para el Tribunal, en un escollo infranqueable, máxime cuando se toman en consideración las especiales exigencias del tratamiento, que solo resulta procedente cuando concurre un interés público esencial.

Como recuerda el TC, el legislador no ha detallado cuáles son las necesidades y los problemas de funcionamiento del sistema democrático que se solventarían mediante la recopilación de datos por los partidos políticos. Esta omisión no puede suplirse apelando al considerando 56 del RGPD[51], pues su contenido es demasiado genérico. Únicamente el legislador está constitucionalmente habilitado para acometer la identificación que clarifique el interés justificativo del tratamiento de datos habilitado. Solo él puede aportar, a través del principio de legalidad, la seguridad jurídica que requiere cualquier posible injerencia en un espacio inicialmente reservado por la Constitución a los derechos fundamentales.

Las disposiciones con un contenido indeterminado y las apelaciones a intereses generales que no se acompañen de razones concretas y garantías específicas no son aceptables. Seguridad y precisión son requisitos ineludibles

[50] STC 76/2019, de 22 de mayo, FJ 7. La jurisprudencia está en consonancia con las exigencias del 52.1 de la CDFUE y del 8.2 del CEDH.

[51] Considerando 56 del RGPD: «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».

si se va a establecer, mediante ley, una habilitación para tratar datos personales.

Más allá de las ausencias reseñadas, en el caso que nos ocupa, es difícil identificar —incluso en abstracto— cuáles pudieran ser los problemas de funcionamiento del sistema electoral español que, por su naturaleza, requieren «la recopilación de datos personales relativos a las opiniones políticas» (art. 58.1 *bis*). Más arduo aún resulta conocer las razones que llevaron al legislador a considerar que permitir a los partidos políticos hacer perfiles personales puede ser un modo conveniente para afrontar las amenazas derivadas del perfilado y condicionamiento de los electores. En definitiva, ¿cómo contribuye esa potestad a hacer frente a actuaciones de empresas como Cambridge Analytica?, ¿en qué ayuda a reaccionar frente a las injerencias de terceros Estados? La respuesta a esta cuestión es el primer paso que deberá afrontar cualquier nuevo intento de regulación de esta materia.

2. LA AUSENCIA DE LIMITACIONES Y DE CERTEZAS

La segunda tacha de inconstitucionalidad que aprecia el Tribunal deriva de la falta de previsión de las condiciones y limitaciones del tratamiento. La habilitación a los partidos políticos para recabar datos personales referentes a las convicciones políticas supone una restricción del derecho a la protección de datos. Por consiguiente, la delimitación de esta injerencia es un mandato insoslayable para el legislador, en la medida en que, como ya se advertía en la STC 292/2000, de 30 de noviembre (FJ 11), «regular esos límites es una forma de desarrollo del derecho fundamental». En efecto, el derecho a la protección de datos también demanda del legislador —y no solo de los particulares y de la Administración— una actitud proactiva que, en su caso, debe proyectarse en su tarea normativa. En su actuación ha de procurar ser lo más preciso y concreto posible, evitando vacíos que puedan permitir prácticas o interpretaciones que pongan en peligro la protección del derecho fundamental del art. 18.4 CE, o de aquellos otros que pudiesen verse concernidos.

El precepto impugnado preveía una única limitación: la recopilación de datos por los partidos políticos solo puede llevarse a cabo «en el marco de sus actividades electorales». El concepto «actividades electorales» resulta notoriamente difuso e indeterminado y no parece que pueda identificarse con el término «período electoral» —mucho más preciso—, que se utiliza en el apdo. 2 del 58 *bis*, pues, de ser así, el legislador no habría empleado una fórmula distinta. Frente a esta indefinición, contrasta, como ya se ha apuntado, la *Data Protection Act* 2018, del Reino Unido. En ella sí se acota el

alcance del término, fijando tanto el marco temporal como las actividades que se pueden desarrollar.

El requerimiento de claridad y previsibilidad es inherente a toda injerencia en un derecho fundamental[52]. La vaguedad e insuficiencia definitoria de la regulación española, unidas a la ausencia de cualquier otra previsión respecto al «alcance y contenido de los tratamientos de datos que autoriza»[53], comportan una ablación de «las exigencias de certeza que han de presidir cualquier injerencia en un derecho fundamental»[54]. Entendiendo esta, en consonancia con la jurisprudencia del TEDH, como la exigencia de normas claras y límites definidos que eviten actos arbitrarios[55]. Para lograrlo, han de preverse tanto el alcance como las modalidades de ejercicio de la facultad reconocida, fijando, por ejemplo, la duración del tratamiento, el tipo de almacenamiento, los usos, quién va a tener acceso a la información o si va a ser utilizada por terceros.

Este mandato se convierte en un imperativo cuando se trata del derecho a la protección de datos, sobre todo en aquellas situaciones en las que actúa con un marcado carácter instrumental, al servicio de la salvaguarda de otros derechos. Un ejemplo claro sería cuando opera en consonancia con el derecho a la intimidad. En esos supuestos, «la protección del derecho fundamental a la intimidad exige que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario»[56].

En nuestro caso, serían el derecho a la libertad ideológica y los derechos de participación política los que demandarían esa diligencia adicional. En el precepto objeto de recurso, las lagunas son tan patentes que el vacío legal es motivo suficiente para apreciar la vulneración del derecho a la protección de

---

52 STEDH, de 4 diciembre de 2008, asunto *S. y Marper contra Reino Unido*, apdo. 99. En la misma línea, STEDH, de 1 julio de 2008, asunto *Liberty y otros contra Reino Unido*, apdo. 62, donde se referencia la doctrina del TEDH acerca de las exigencias de previsibilidad de la ley.

53 STC 76/2019, de 22 de mayo, FJ 7.

54 STC 76/2019, de 22 de mayo, FJ 7.

55 STEDH, de 29 de junio de 2006, asunto *Weber y Saravia contra Alemania*, apdos. 93-95.

56 Apdo. 39 de la STJUE, de 7 de noviembre de 2013, asunto *IPI*, C-473/12, ECLI:EU:C:2013:715; en el mismo sentido, STJUE, de 16 de diciembre de 2008, *Satakunnan Markkinapörssi y Satamedia*, C73/07, ECLI:EU:C:2008:727, apdo. 56; STJUE, de 9 de noviembre de 2010, *Volker und Markus Schecke y Eifert*, C92/09 y C93/09, ECLI:EU:C:2010:662, apdos. 77 y 86.

datos. Por ello, el Tribunal Constitucional concluye que el apdo. 1 del 58 *bis* LOREG también vulnera el derecho fundamental por haber abdicado de su obligación de dotar de previsibilidad y certeza a la configuración legal del derecho a la protección de datos.

No obstante, si el legislador decidiera abordar en el futuro esta cuestión, al perfilar y delimitar qué tratamientos se van a permitir, durante cuánto tiempo y para qué finalidades, ha de tener en cuenta que, en este caso, además del derecho a la protección de datos, hay otros derechos fundamentales en concurso susceptibles de ser vulnerados. Un riesgo adicional que no puede obviarse.

3. LA FALTA DE GARANTÍAS TAMBIÉN ES UN MODO DE VULNERAR EL DERECHO A LA PROTECCIÓN DE DATOS

Es doctrina reiterada del Tribunal Constitucional[57], también del Tribunal de Justicia de la Unión Europea[58] y del Tribunal Europeo de Derechos Humanos[59], que el derecho a la protección de datos se ve afectado, con una «gravedad similar a la que causarían intromisiones directas»[60], por la omisión de las cauciones y medidas de protección adecuadas.

El TEDH, en el asunto *S. y Marper contra Reino Unido*, utiliza los principios del tratamiento de datos como parámetro interpretativo mediante el que determinar si una determinada previsión normativa ofrece garantías

---

57 SSTC 292/2000, de 30 de noviembre, FJ 10; STC 143/1994, de 9 de mayo, FJ 7, y 254/1993, de 20 de julio, FJ 4.

58 La ausencia de garantías es uno de los elementos clave que llevaron al TJUE a declarar la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Véase STJUE (Gran Sala), de 8 de abril de 2014, *Digital Rights Ireland Ltd*, asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238, apdo. 54. Sobre la relevancia de esta sentencia y el derecho a la protección de datos reconocido en la Carta de Derechos Fundamentales de la Unión Europea, véase López Aguilar (2017).

59 El TEDH, asumiendo que hay un cierto margen de actuación por parte de los Estados, advierte que hay garantías que son imprescindibles para la evitar abusos en los elementos esenciales de los derechos fundamentales. En este sentido, véase, la Sentencia TEDH, de 5 septiembre de 2017, asunto *Barbulescu contra Rumanía*, apdos. 119 a 121.

60 STC 76/2019, de 22 de mayo, FJ 7.

suficientes (González Fuster, 2009: 632). De modo que, para cumplir con esta exigencia, la regulación legal del tratamiento ha de asegurar, al menos, que «los datos sean pertinentes y no excesivos en relación a las finalidades […] y que se conserven durante un período de tiempo que no exceda del necesario […]. […] ha de contener también garantías que protejan eficazmente los datos de carácter personal registrados contra los usos imprevistos y abusivos»[61]. Cuando el tratamiento afecta a categorías especiales de datos, es inexcusable que la legislación no contemple estos elementos[62].

El apdo. 1 del 58 *bis* no cumple con ninguno de estos requisitos. Ni del artículo objeto de enjuiciamiento, ni mucho menos del «sentido de la enmienda de adición de la que trae causa»[63], se desprende la existencia de un marco apropiado de garantías. Tampoco es posible inferirlas de las normas básicas que configuran el régimen de la protección de datos (RGPD y LOPDGDD). Esta última cuestión requiere de una explicación más pormenorizada, sin perjuicio de dedicar, siquiera unas líneas, a apuntar las razones que llevan al Tribunal a descartar otros motivos de impugnación también planteados.

El art. 58 *bis* se limita a reseñar la necesidad de reconocer y disponer «las garantías adecuadas». El legislador renuncia expresamente a detallarlas en el cuerpo de la ley, aunque fuese de forma meramente orientativa. Esa renuncia no puede suplirse mediante otras iniciativas, como la llevada a cabo mediante la Circular 1/2019. «La AEPD […] no es la vía para hacer lo que le corresponde al legislador» (Arenas Ramiro, 2019: 371). Diferir a una circular de la AEPD el establecimiento de las garantías adecuadas supone «una deslegalización que sacrifica la reserva de ley *ex* art. 53.1 CE»[64].

Es la reserva de ley la razón que lleva al Tribunal Constitucional a declarar, aun reconociendo su valor hermenéutico, que las enmiendas presentadas en la tramitación parlamentaria del art. 58 *bis* «no pueden suplir o sanar las insuficiencias constitucionales»[65] de la norma objeto de recurso.

Finalmente, la posibilidad de colmar la ausencia de garantías del precepto acudiendo a las previsiones del RGPD y de la LOPDGDD también ha de ser descartada. Tanto la remisión a dichas normas, como la identificación de los

---

61 STEDH, de 4 diciembre de 2008, asunto *S. y Marper contra Reino Unido*, apdo. 103.

62 Si bien en este caso los datos sensibles afectados serían los relativos a las opiniones políticas, es perfectamente trasladable la doctrina establecida por el TEDH para los datos relativos a la salud en la STEDH, de 25 de febrero de 1997, asunto *Z c. Finlandia*, apdos. 95-96, y STEDH, de 17 de octubre, *I. c. Finlandia*, apdos. 38-40.

63 STC 76/2019, de 22 de mayo, FJ 8.

64 STC 76/2019, de 22 de mayo, FJ 8.

65 STC 76/2019, de 22 de mayo, FJ 8.

artículos concretos que contendrían dichas garantías se realizaron por el legislador de manera implícita, con la consiguiente inseguridad e indeterminación, inasumibles cuando lo que está en juego es la protección de un derecho fundamental.

Con todo, y con el propósito de despejar toda duda, el Tribunal se adentra en esta cuestión, «a efectos dialécticos»[66], concluyendo que el precepto no identifica las reglas que deben aplicarse. Esto es, de todo el marco normativo que conforman el RGPD y la LOPDGDD, no se precisa cuáles serían las garantías que regirían el tratamiento de las opiniones políticas por los partidos. Es decir, no había un marco de actuación y garantía definido para el tratamiento que el apdo. primero del art. 58 *bis* habilitaba.

Profundizando en la cuestión, el Tribunal constata que el RGPD solo «establece las garantías mínimas comunes o generales para el tratamiento de datos personales que no son especiales». Por su parte, la LOPDGDD ni siquiera cuenta con un precepto en el que, de manera singularizada y específica, se discipline el tratamiento de los datos ideológicos. Tampoco figura en dicha ley pauta normativa alguna, a diferencia de lo que acontece, por ejemplo, en la normativa alemana sobre la materia, en la que se dispone de un marco general de garantías específico para las categorías especiales de datos[67]. En definitiva, al no preverse las cauciones pertinentes y adecuadas se vulnera el contenido esencial del derecho.

De este pronunciamiento del TC pueden extraerse, al menos, tres elementos definitorios del derecho a la protección de datos personales. En primer lugar, es un derecho dotado de un alto nivel de formalidad, lo que se refleja en la exigencia constitucional de una actuación positiva y proactiva por parte del legislador (fijando el marco de garantías, pero también los límites y la finalidad del tratamiento).

En segundo lugar, la necesidad de adecuar el marco de garantías a las particularidades del tratamiento y la naturaleza de los datos supone, en última instancia, que una parte del contenido del derecho siempre tendrá un componente funcionalmente variable, conformando una especie de contenido esencial de contexto. Una circunstancia muy particular y a la que deberá prestar especial atención el legislador, pues solo así podrá mantener unos niveles de garantía y protección del derecho adecuados. Tendrá que fijar, para cada caso, la regulación más apropiada para lograr los fines del tratamiento sin incurrir en la vulneración de este.

---

66 STC 76/2019, de 22 de mayo, FJ 8.

67 Sección 48 de la ley de protección de datos alemana. Pueden consultarse versiones en alemán e inglés de la *Bundesdatenschutzgesetz* en: https://bit.ly/36YLlyy (última consulta: 14-12-2020).

Finalmente, el acomodamiento de las garantías —y los límites— a las circunstancias específicas del tratamiento es una labor que, por afectar a la delimitación de los elementos nucleares del derecho, solo puede ser ejecutada por el legislador. Por lo tanto, cualquier eventual omisión no podrá ser ulterior y hermenéuticamente integrada mediante la técnica de la interpretación conforme.

4. INCONSTITUCIONAL Y NULO

En un panorama como el descrito, que descarta cualquier posibilidad de interpretación conforme (incompatible con la apuntada naturaleza formal y prescriptiva del derecho), la conclusión del Tribunal no podía ser otra: el precepto impugnado es contrario a la Constitución, ya que vulnera el derecho a la protección de datos. En palabras del Tribunal: «[La] ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama» (FJ 9).

En definitiva, el precepto objeto de recurso supone una injerencia injustificada (por no identificarse la finalidad), desproporcionada (por la ausencia de límites claros) y carente de las mínimas garantías en la regulación de un derecho fundamental, de la que solo se puede inferir (art. 18.4 en su conexión con el 53.1, ambos de la CE) la inconstitucionalidad y, por tanto, nulidad del apdo. 1 del art. 58 *bis* objeto de recurso.

Un artículo que, a tenor de lo que indica la enmienda de la que trae causa, pretendía enfrentar los riesgos que determinados usos y prácticas suponen para los procesos electorales. Sin embargo, si ese era el objetivo real, habría «requerido una mayor reflexión […] para redactar el precepto de una manera plenamente respetuosa con los intereses en juego. […] [Especialmente, si se tiene] en cuenta […] el conflicto de interés concurrente en la elaboración de la disposición» (Pascua Mateo, 2019: 558).

IV. EN TORNO A LA NECESIDAD DE ESTABLECER UN MARCO DE GARANTÍAS PARA EL TRATAMIENTO DE DATOS ESPECIALES. REFLEXIONES Y PROPUESTAS

El Tribunal Constitucional ha resuelto, con celeridad, la problemática suscitada en torno al tratamiento de las convicciones políticas de los electores por parte de las formaciones políticas. En su pronunciamiento aplica, de manera sistemática

y coherente, tanto su doctrina sobre el contenido esencial del derecho a la protección de datos[68] como los aspectos referentes a la reserva de ley[69], profundizando en la particular naturaleza formal del derecho previsto en el art. 18.4 CE.

En la fundamentación de la sentencia se hace una importante advertencia, que no ha de ser soslayada, respecto del régimen jurídico aplicable a los datos especiales. Recuerda el Alto Tribunal que, el RGPD, no configura un régimen específico para los datos especiales y, «por ende, tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles»[70].

Con esta afirmación, el Tribunal está poniendo sobre la mesa un delicado asunto no resuelto por el legislador nacional de forma completa. Es cierto que, en la LOPDGDD, se desarrollan algunas garantías y exigencias adicionales para el tratamiento de los datos especiales. La más reseñable es la, ya apuntada, invalidez del consentimiento como base de legitimación en aquellos tratamientos «cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico» (art. 9.1 LOPDGDD). Además de esa previsión general, en la disposición adicional decimoséptima consta un régimen más detallado para aquellos tratamientos en los que se utilizan datos de salud (y los genéticos cuando sean utilizados en investigación y prevención de la salud). Ahora bien, dejando a salvo lo previsto en esos preceptos —importante, aunque insuficiente—, el problema que se atisba a futuro se antoja, ciertamente, complejo.

Ni el legislador europeo, ni tampoco el nacional, han afrontado el tratamiento de las categorías especiales con el debido nivel de detalle. En efecto, estando previstas en el art. 9.2 RGPD las circunstancias en que los datos especiales pueden tratarse —existencia de base de legitimación para ello mediante—, sin embargo, no se han regulado las garantías específicas que demanda el contenido esencial del derecho.

Como puede constatarse, no todos los tratamientos en los que se utilizan datos de las categorías especiales cuentan con una ley sectorial que los regule y, menos aún, que incorpore garantías específicas. Por otra parte, las leyes existentes se limitan a hacer referencias generales a la necesidad de observancia de la normativa de protección de datos, sin establecer mayores cautelas o precisiones, salvo alguna notable excepción como la Ley 20/2011, de 21 de julio, del Registro Civil[71].

---

68 Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

69 Sentencias del Tribunal Constitucional 49/1999, de 5 de abril, FJ 4, y 154/2014, de 22 de septiembre, FJ 7.

70 STC 76/2019, de 22 de mayo, FJ 8.

71 Aunque el preámbulo hace referencia a la ya derogada Ley de Protección de Datos de 1999, no es menos cierto que regula previsiones específicas para los datos especiales.

Ante esta situación heterogénea, parece apropiado que, conforme se vayan detectando carencias en las diferentes normativas sectoriales, que, de un modo u otro, disciplinen algún tipo de tratamiento de datos, se proceda a incorporar a su articulado previsiones que aseguren el nivel de garantía y de detalle que la reserva de ley requiere. Esta necesidad de actualización, por otra parte, casi es un imperativo derivado de la constante evolución de los avances tecnológicos en la materia.

Todo ello conduce a pensar que, en un futuro, la elaboración de leyes relativas a datos personales debería acompañarse de un estudio de impacto del tipo de datos que puedan llegar a tratarse, así como de un régimen de garantías adecuado a los tratamientos que puedan producirse.

Cumple no olvidar que el legislador debe ofrecer, en relación con este derecho, un plus de seguridad jurídica a los ciudadanos, habilitando un marco de garantías mucho más sólido y al que las normas sectoriales pudieran remitirse. De este modo, se colmarían las eventuales lagunas que pudiesen existir en la regulación sectorial en vigor y, a la vez, se reforzarían las previsiones que, de manera específica, dispusiese el legislador. En definitiva, se dotaría al modelo de mayor certeza y previsibilidad.

Adicionalmente, sería conveniente incorporar ciertas garantías generales para el tratamiento de datos especiales en la LOPDGDD —aunque resulte un tanto extraño modificar una ley que no tiene ni tres años de vida—. El modelo alemán, con un régimen de garantías singularizado para las categorías especiales de datos —sin perjuicio de las específicas sectoriales— puede ser una buena referencia[72].

Sería un error considerar que los problemas de fondo abordados por la sentencia quedan resueltos con la declaración de inconstitucionalidad del precepto enjuiciado. Regular los tratamientos de datos personales por parte de los partidos políticos, singularmente los referidos a las opiniones políticas, es una imperiosa necesidad. Como advirtiera García Mahamut años antes de este conflicto, «la realidad se muestra tozuda y habrá que prepararse para afrontar la existencia de bases de datos por parte de los partidos que capturarán información sobre los votantes de una variedad de fuentes importantes. Ello se pondrá a disposición de campañas personalizadas y dirigidas a concretos segmentos del electorado» (2015: 336). Frente a la inexorabilidad de lo fáctico, habrán de adoptarse medidas y se tendrá que determinar hasta qué punto se quieren aprovechar las posibilidades que la

[72] Véase la sección 48 de la ley de protección de datos alemana. Pueden consultarse versiones en alemán e inglés de la *Bundesdatenschutzgesetz* en: https://bit.ly/36YLlyy (última consulta: 14-12-2020).

tecnología ofrece. Clarificar los límites a esa actividad es un reto ineludible para garantizar la observancia de los derechos fundamentales que puedan verse afectados.

Por tal motivo, una futura regulación del tratamiento de las opiniones políticas por los partidos debería tomar en consideración las lecciones que se desprenden de la sentencia que se comenta. Si a esas enseñanzas les sumamos los muchos elementos aprovechables de la Circular 1/2019 de la AEPD, las recomendaciones realizadas en el Dictamen 3/2018 del Supervisor Europeo de Protección de Datos[73] y las aportaciones que, en cuanto al régimen sancionador, realiza el Reglamento (UE, Euratom) 2019/493 del Parlamento Europeo y del Consejo, de 25 de marzo de 2019[74], el legislador contará con bases sólidas sobre las que articular la necesaria regulación del tratamiento de datos personales referidos a opiniones políticas. Incluso podría, como herramienta complementaria del régimen que legalmente se estableciese, disponerse en la propia ley que los partidos políticos adoptasen «otros mecanismos previstos legamente […] [como son] los llamados códigos de conducta» (Arenas Ramiro, 2019: 368).

No quisiera concluir este análisis sin incidir en lo apremiante de abordar, de manera decidida, las carencias de la normativa de protección de datos en lo referente a la regulación de los datos especiales. El constante aumento de la capacidad para generar nuevas informaciones y datos personales, mediante la combinación de algoritmos, inteligencia artificial y *big data*, hace perentorio afrontar esta cuestión. En efecto, ya existen tratamientos que, partiendo de datos no pertenecientes a alguna de las categorías especiales o, incluso, sin llegar a utilizar datos personales en absoluto —por basarse en datos anonimizados—, son capaces de suministrar informaciones que, al menos potencialmente, sí son merecedoras de una especial protección. Sin embargo, el ordenamiento jurídico no ofrece, actualmente, una respuesta sólida y articulada. Si queremos seguir sosteniendo los estándares de seguridad jurídica hasta ahora establecidos para la defensa de los derechos fundamentales, si se quiere que el modelo europeo de protección de datos siga siendo una referencia por sus garantías, ha de cerrarse cuanto antes esa vía de agua.

---

[73] *Opinion 3/2018, EDPS Opinion on online manipulation and personal data*. Puede consultarse en: https://bit.ly/3cYNFt1 (última consulta: 14-12-2020).

[74] Reglamento destinado a «proteger la integridad del proceso democrático europeo estableciendo sanciones financieras en situaciones en las que los partidos políticos europeos o las fundaciones políticas europeas se aprovechen de infracciones de las normas de protección de datos personales con el fin de influir en el resultado de las elecciones al Parlamento Europeo» (considerando 3).

BIBLIOGRAFÍA

Adsuara Varela, B. (2019). El «perfilado ideológico» de los ciudadanos por los partidos políticos. *Consultor de los ayuntamientos y de los juzgados*, 3, 77-89.

Arenas Ramiro, M. (2019). Los políticos, opiniones políticas e Internet: la lesión del derecho a la protección de datos personales. *Teoría y Realidad Constitucional*, 341-372. Disponible en: https://doi.org/10.5944/trc.44.2019.26005.

García Herrero, J. (2019). Tratamiento de datos en actividades electorales (Disposición final tercera). En J. López Calvo (coord.). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 295-321). Madrid: Bosch.

García Mahamut, R. (2015). Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español. *Teoría y Realidad Constitucional*, 35, 309-338. Disponible en: https://doi.org/10.5944/trc.35.2015.14921.

García Sanz, R. M. (2019). Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público. *Revista de Estudios Políticos*, 183, 129-159. Disponible en: https://doi.org/10.18042/cepc/rep.183.05.

González Fuster, G. (2009). TEDH – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Artículo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas. *Revista de Derecho Comunitario Europeo*, 33, 619-633.

Lassalle, J. M. (2019). *Ciberleviatán*. Barcelona: Arpa.

Lazer, D., Kennedy, R., King, G. y Vespignani, A. (2014). Big data. The parable of Google Flu: traps in big data analysis. *Science (New York, N.Y.)*, 343 (6176), 1203-1205. Disponible en: https://doi.org/10.1126/science.1248506.

López Aguilar, J. F. (2017). La protección de datos personales en la más reciente jurisprudencia del TJUE: Los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU. *Teoría y Realidad Constitucional*, 39, 557-581. Disponible en: https://doi.org/10.5944/trc.39.2017.19165.

Medina Guerrero, M. (2019). Categorías especiales de datos. En A. Rallo Lombarte (dir.). *Tratado de protección de datos actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 251-273). Valencia: Tirant lo Blanch.

Pascua Mateo, F. A. (2019). Un nuevo capítulo en la tutela del derecho a la protección de datos personales: Los datos de contenido político. Comentario a la sentencia del Tribunal Constitucional 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019. *Revista de Las Cortes Generales*, 106, 549-558. Disponible en: https://doi.org/10.33426/rcg/2019/106/1411.

Puente Escobar, A. (2019). Principios y licitud del tratamiento. En A. Rallo Lombarte (dir.). *Tratado de protección de datos actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 115-168). Valencia: Tirant lo Blanch.

Salas Carceller, A. (2014). El concepto de interés público: distinta visión del Tribunal Constitucional y del Tribunal Supremo. *Revista Aranzadi Doctrinal*, 1, 117-123.

Suárez-Gonzalo, S. (2018). 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*, 21 (44), 27-36.

Torres Soriano, M. R. (2017). Hackeando la democracia: operaciones de influencia en el ciberespacio. *Bie3*, 6, 826-839.

Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Villalobos Guízar, V. (2018). Cambridge Analytica: De la interfaz al régimen. *Revista de La Universidad de México*, 5, 131-135.

Wachter, S. y Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2, 1-130. Disponible en: https://doi.org/10.31228/osf.io/mu2kf.

Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, 47 (4), 995-1020. Disponible en: https://ssrn.com/abstract=3022646.