



**VNiVERSIDAD
D SALAMANCA**

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

DOBLE GRADO EN DERECHO Y ADE

Derecho Constitucional

Democracia, representación, participación y partidos políticos

Curso 2019/2020

¿PUEDEN LOS PARTIDOS POLÍTICOS ACCEDER A LOS DATOS IDEOLÓGICOS DE LOS CIUDADANOS EN LA RED?

ALEJANDRA PRADO CABRILLO

TUTORA: M^a MERCEDES IGLESIAS BÁREZ

JUNIO 2020

TRABAJO FIN DE GRADO
DOBLE GRADO EN DERECHO Y ADE

Derecho Constitucional

Democracia, representación, participación y partidos políticos

**¿PUEDEN LOS PARTIDOS
POLÍTICOS ACCEDER A LOS DATOS
IDEOLÓGICOS DE LOS
CIUDADANOS EN LA RED?**

**ARE POLITICAL PARTIES ABLE TO
ACCESS TO THE CITIZENS'
IDEOLOGICAL DATA ON THE NET?**

Alejandra Prado Cabrillo
apcabrillo@usal.es

Tutora: M^a Mercedes Iglesias Bárez

RESUMEN

El avance de internet y el desarrollo tecnológico han creado un nuevo canal de comunicación, entre otros sectores, en el de la política, donde votantes y grupos políticos interactúan, generando un concepto de sociedad y de democracia desconocidos hasta la fecha. No todo son aspectos positivos, ya que el auge de las redes sociales supone, a su vez, una intromisión en los derechos fundamentales de los ciudadanos, concretamente en la protección de los datos personales, cuando estos datos no se tratan ni se obtienen de manera adecuada, siendo además, utilizados para fines ilícitos.

Con ánimo de regular las novedosas situaciones que pueden generarse a raíz de estos avances, se introdujo el artículo 58 bis en la Ley Orgánica del Régimen Electoral General. La finalidad era evitar que se repitan casos en los que se usan los datos extraídos de los perfiles en redes sociales de los ciudadanos con el objetivo influenciar su intención de voto. Finalmente, este artículo ha sido declarado inconstitucional en la STS 76/2019 por su injerencia en ciertos derechos fundamentales y su inobservancia de las garantías debidas para el tratamiento y obtención de dichos datos.

PALABRAS CLAVE: Democracia, protección, datos, derechos fundamentales, inconstitucional, partidos políticos

ABSTRACT

Internet progress and technological development has created a new communication channel, among others, on the political sphere, where voters and political parties interact, generating a society and democracy concept that were unknown until now. Not everything is positive, since the rise of social networks means, in turn, an intromission on the citizens' fundamental rights, concretely on the personal data protection right, when these data are not handled nor obtained appropriately, besides, being used in illicit purposes.

With the aim of regulate the original situations which could be produced by these advances, the article 58 bis was introduced on the Organic Law of the General Electoral Procedure. The purpose was to avoid cases in which the data received from the social media were used with the objective of influencing people's vote intention. Finally, this article has been declared unconstitutional on the Supreme Court Judgement 76/2019 due to its fundamental rights interference and its breach on the guarantees needed on the treatment of those data.

KEYWORDS: Democracy, protection, data, fundamental rights, unconstitutional, political parties

ÍNDICE

ÍNDICE DE ABREVIATURAS	1
INTRODUCCIÓN.....	1
CAPÍTULO 1: LA CIBERDEMOCRACIA Y LA PROTECCIÓN DE DATOS.....	3
1.1. Terminología y concepto	3
1.2. Nuevas denominaciones para la democracia de las Nuevas Tecnologías.....	4
1.2.1. <i>Democracia electrónica</i>	4
1.2.2. <i>Ciberdemocracia</i>	5
1.2.3. <i>Democracia digital</i>	5
1.2.4. <i>Aclaraciones conceptuales</i>	5
1.3. El uso de las NTIC por parte de los partidos políticos.....	6
1.3.1. <i>Riesgos del uso de las NTIC</i>	8
1.3.2. <i>Conflicto entre las NTIC y la protección de datos</i>	9
CAPÍTULO 2: RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS POLÍTICOS.....	11
2.1. Régimen jurídico a nivel comunitario.....	11
2.2. Régimen jurídico del Consejo de Europa	17
2.3. Régimen jurídico a nivel nacional.....	21
CAPÍTULO 3: ANÁLISIS DE LA SENTENCIA 76/2019 DEL TRIBUNAL CONSTITUCIONAL	25
3.1. Fin legítimo	27
3.2. Condiciones determinadas.....	28
3.3. Garantías adecuadas	30
CONCLUSIONES.....	32
BIBLIOGRAFÍA.....	35
Libros, artículos y revistas	35
Legislación, jurisprudencia y otros instrumentos.....	37

ÍNDICE DE ABREVIATURAS

AEPD – Agencia Española de Protección de Datos

GT29 – Grupo de Trabajo del Artículo 29

JEC – Junta Electoral Central

LOPDGDD – Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

LOREG – Ley Orgánica del Régimen Electoral General

NTIC – Nuevas Tecnologías de la Información y la Comunicación

PSOE – Partido Socialista Obrero Español

RGPD – Reglamento General de Protección de Datos

SEPD – Supervisor Europeo de Protección de Datos

STC – Sentencia del Tribunal Constitucional

TC – Tribunal Constitucional

INTRODUCCIÓN

El presente trabajo tiene por objeto el análisis de la situación actual del derecho a la protección de datos personales, centrándonos en aquellos de carácter especialmente sensibles, para terminar examinando los motivos que han llevado al Tribunal Constitucional a declarar la inconstitucionalidad del apartado primero del artículo 58 bis introducido en la Ley Orgánica del Régimen Electoral General¹, a propuesta del PSOE².

El interés por la protección de los datos personales no es algo nuevo, sino que ya viene reconocido en la Constitución Española como uno de los derechos que merecen una especial defensa, en el capítulo segundo sección primera relativo a los derechos fundamentales. Este derecho lo encontramos concretamente en el artículo 18.4 de dicho texto, pero como veremos, está amparado por un amplio marco legislativo con la intención de garantizar su seguridad e inviolabilidad.

La sociedad avanza, y con ella los nuevos métodos de obtención y tratamiento de datos, por lo que algunos de los mecanismos tradicionales de protección han quedado obsoletos

¹ A partir de ahora LOREG

² Partido Socialista Obrero Español

y se hace necesario un desarrollo legislativo eficaz que contemple estas nuevas técnicas. Con el auge de internet y, sobre todo, de las redes sociales, resulta inevitable el acceso a los datos más íntimos de los ciudadanos, ya que son ellos mismos quienes los exponen en sus perfiles a través de sus publicaciones o interacciones con otros usuarios. Esto implica que aquellos interesados en extraer estos datos y utilizarlos con fines no siempre lícitos tengan una fuente directa e inagotable de información.

Poco a poco las nuevas tecnologías han ido calando en el ámbito político y ya podemos ver como diversas organizaciones políticas cuentan con perfiles en distintas redes sociales para comunicarse de manera más directa con sus electores o con la comunidad. Esto ha creado una nueva sociedad y una nueva forma de entender la democracia que trata de superar las deficiencias tradicionales acercando la política a los ciudadanos.

Este interés por los datos que las personas emiten en sus cuentas personales, se ve incrementado cuando se trata de opiniones e ideologías políticas, ya que permiten la creación de perfiles individuales de electores. Lo que se pretende evitar es el libre acceso y tratamiento de estos datos por parte de los partidos políticos con la intención de influenciar y pervertir su intención de voto.

En esta línea, el PSOE, a través de la enmienda 331, introdujo un nuevo artículo en la LOREG que, precisamente, tenía como objetivo legislar en esta materia. La introducción de este precepto fue muy controvertida a pesar de que se aprobó por una amplia mayoría parlamentaria y terminó declarándose inconstitucional por el Tribunal Constitucional, en la Sentencia 76/2019, a raíz de un recurso interpuesto por el Defensor del Pueblo avalado por un gran número de Asociaciones de Protección de Datos.

Teniendo esto en cuenta, en el trabajo se abordarán los nuevos conceptos de democracia y la influencia de las Nuevas Tecnologías de la Información y de la Comunicación en la sociedad, además de su uso por parte de los partidos políticos, desentrañando los riesgos que esto presenta y el conflicto que suponen con el derecho de protección de datos.

Por otro lado, haremos un repaso de toda la legislación vigente sobre esta materia en función de su alcance para así crear un contexto normativo. Finalmente, analizaremos el por qué y los argumentos esgrimidos por el Tribunal Constitucional que le han llevado a declarar inconstitucional el precepto introducido por el Grupo Parlamentario Socialista.

CAPÍTULO 1: LA CIBERDEMOCRACIA Y LA PROTECCIÓN DE DATOS

1.1. Terminología y concepto

En las últimas décadas se han ido sucediendo numerosos avances en el plano de las Nuevas Tecnologías de la Información y la Comunicación, tomando como punto álgido los años 90 con la expansión de internet. Desde entonces, se han continuado los debates entre los analistas sobre las implicaciones que estas nuevas herramientas aplicadas al ámbito político conllevarían en las democracias occidentales.

A pesar de los numerosos estudios, no se ha llegado a acuñar un término unánime para referirse a las Nuevas Tecnologías de la Información y la Comunicación en el ámbito político, de tal manera que conviven vocablos tales como: “democracia virtual”, “democracia digital”, “ciberdemocracia”, “democracia electrónica”, “política virtual”, “teledemocracia” o “república electrónica”, entre otras expresiones, para aludir a la misma realidad.

Algunos ejemplos del uso indistinto de estos términos los encontramos en Cairo Carou³, que se decanta por la utilización de “democracia electrónica” y “ciberpolítica” para referirse a la transformación del espacio de la política, apuntando que el ciberespacio ha transformado los viejos espacios de acción política, donde éstos ya no dependen de la ubicación geográfica, sino que más bien son espacios de flujos. O en el caso de Subirats, que habla de “democracia electrónica” o “ciberdemocracia”, ambas expresiones aludiendo al mismo concepto: *la utilización de las TIC – principalmente en internet – en los procesos políticos democráticos de las comunidades locales, estatales, regionales, nacionales o globales. Las TIC son utilizadas en este sentido por parte de los gobiernos, los partidos políticos, los grupos de interés, las organizaciones de la sociedad civil, las organizaciones gubernamentales internacionales y los ciudadanos*⁴.

³ GARCÍA JIMÉNEZ, L. DEL, “Reseña de “Democracia digital. Límites y oportunidades” de Cairo Carou, H.”.

⁴ COLOMBO, C. DEL “Innovación democrática y TIC, ¿hacia una democracia participativa?”, *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 2006, p.29.

Para poder hablar de e-democracia, antes tenemos que abordar la e-ciudadanía, que se refiere a una nueva ola de derechos sociales o derechos digitales⁵. La e-ciudadanía supone un enfoque que apunta a impulsar formas participativas en las políticas y gestiones cotidianas, donde la ciudadanía interviene diferenciada en grupos que aúnan unos intereses “concretos”. La existencia de la e-ciudadanía supone una reconsideración del tiempo y una desterritorialización del espacio, lo que se traduce en relaciones más flexibles y desvinculadas, lo que favorece la relación de las comunidades virtuales. Se puede constituir una comunidad en el momento en el que se establece una relación en la que se comparten gustos, aficiones, emociones, preocupaciones o intereses por un determinado tema⁶.

1.2. Nuevas denominaciones para la democracia de las Nuevas Tecnologías

Como ya se ha mencionado, coexisten numerosos términos para referirse a la misma realidad, pero en este apartado se va a realizar una especial mención a las locuciones más utilizadas por los analistas, siendo éstas, “democracia electrónica”, “democracia digital” y “ciberdemocracia”.

1.2.1. Democracia electrónica

La “democracia electrónica” o “e-democracia” – abreviatura del término inglés “electronic democracy” – se define como un modelo de democracia que trata de mejorar las comunicaciones entre el gobierno y los ciudadanos, pero de una manera individualizada. Consistiría en mejorar los cauces de comunicación esporádica, implementando mecanismos instrumentales que los representantes ponen a disposición de los ciudadanos para aumentar la participación ciudadana. Un ejemplo sería el voto, que se convertiría en el voto electrónico, o en caso de referéndum, que sería referéndum electrónico.

⁵ KAUFMAN, E. DEL, E-Ciudadanía, prácticas de Buen Gobierno y TIC, 2005.

⁶ MARTÍNEZ RODRÍGUEZ, J. DEL, “Participación política, democracia digital y e-ciudadanía para el protagonismo de adolescentes y jóvenes”, *Revista electrónica interuniversitaria de formación del profesorado*, 2011, vol. 37, no 14-2, p. 19-33.

1.2.2. Ciberdemocracia

La ciberdemocracia utópica hace referencia a un modelo de democracia directa basado en comunidades virtuales autogestionadas en el ciberespacio, sin necesidad de la intermediación de las instituciones representativas; mientras que, también se acuña el término ciberdemocracia viable, que se refiere a una participación ciudadana plural mediante aportaciones generadas gracias a las NTIC, que más tarde los representantes acabarían incorporando a sus acciones.

1.2.3. Democracia digital

Con “democracia digital”, nos referimos a un término más exacto que el de “democracia electrónica”, ya que el adjetivo “electrónico” podría hacer también referencia al uso de la televisión.

Partiendo de esa aclaración, la “democracia digital” es una herramienta adicional a las prácticas políticas tradicionales a través de las NTIC y no un reemplazo de ellas. Nace con el objetivo de reparar las deficiencias del sistema actual.

La democracia digital requiere que el Estado promueva herramientas de participación, como foros de discusión, para que los ciudadanos puedan intercambiar información política y deliberar a través de los nuevos medios con el objetivo de aumentar la deliberación en el discurso político mediante una participación creciente.

1.2.4. Aclaraciones conceptuales

La utilización de las NTIC, entre otros motivos, ha supuesto que las administraciones quieran darse a conocer como organizaciones modernas e inclusivas de los adelantos tecnológicos, y por ello se presenten noticias de innovaciones comunicativas como si se tratase de adelantos en la esfera de la democracia digital. Por tanto, la inauguración de oficinas virtuales que faciliten diversos servicios para evitar a los usuarios el traslado, serían considerados como avances en la ciberdemocracia, sin embargo, a pesar de ser avances positivos, son en realidad innovadores en la “e-administración”, donde el ciudadano está considerado consumidor de servicios públicos. En consecuencia, conviene

definir de una manera breve qué se debería entender al emplear algunas palabras relacionadas con las NTIC en el contexto político⁷ según Garrido et al., (2010):

e-democracia: Hace referencia a un proceso en el que se incorporan las NTIC a las actividades político-ciudadanas, donde se incentiva el debate para llegar a una solución consultada de problemas de gobernabilidad que afectan a los ciudadanos de un sistema político democrático representativo.

e-voting: Este término se refiere a dos procesos: el primero consiste en la sustitución del papel por tableros electrónicos o tarjetas perforadas en los locales de votación o, el segundo, al envío de formularios a través de dispositivos como los teléfonos u ordenadores. Este segundo proceso sustituye al acto físico de acudir a las urnas a emitir el voto presencial a la acción de realizarlo a distancia.

e-governance: Incluye el ejercicio del poder mediante la incorporación gradual y sistemática de plataformas de comunicación digital. Busca incrementar la participación ciudadana de tal forma que se desarrolla una actitud más crítica y reflexiva que se traduce en una mayor actividad que favorece la democracia representativa utilizando las NTIC en los procesos políticos.

Nos encontramos con otras locuciones como son la e-administración, el e-government o la e-participación, todos ellos haciendo referencia a procesos administrativos en los que mayormente se incluye a la ciudadanía y que de manera errónea se usan en contextos políticos.

1.3. El uso de las NTIC por parte de los partidos políticos

Las NTIC han supuesto un gran avance para la sociedad en muchos aspectos, entre ellos el político, donde los gobernantes no han tardado en adoptarlas rápidamente ya que en ellas han visto la posibilidad de acceder a los ciudadanos de una manera directa sin tener que recurrir a los medios tradicionales.

⁷ GARRIDO CABEZAS, N. DEL. La construcción de una democracia digital, *Revista Latina*, 2010, p.5. http://www.revistalatinacs.org/10SLCS/actas_2010/032_Norman.pdf

Después de las elecciones generales de España el 26 de junio del 2016, un equipo del Centro de Investigaciones Sociológicas del gobierno preguntó a los ciudadanos si estaban satisfechos con la democracia. Cuando se pidió valorar las instituciones democráticas, el 24,2% respondió que “no confiaba nada” en los partidos políticos⁸. Varios autores⁹ han descrito la crisis de la desafección democrática que atraviesan los países europeos: los ciudadanos no se sienten representados, el voto es considerado poco útil y el ausentismo electoral no disminuye¹⁰.

En este contexto, las NTIC aparecen como una alternativa para que los políticos consigan legitimidad, ya sea a través de consultas electrónicas, ofertas de trámites en línea y desclasificación de documentos. En palabras de Lévy, las NTIC podrán llegar a producir una “*ciberdemocracia planetaria*” que traerá “*paz, libertad y prosperidad para el género humano*”¹¹.

Entre algunas de las medidas se encuentra el diseño de páginas web por parte de los partidos políticos, por las que se dirigen a la ciudadanía a través de continuas publicaciones sobre actualidad o novedades en el partido, de manera que los afiliados y el resto de la comunidad que quiera acceder a estas noticias, podrá hacerlo. Es una forma de acercarse a los ciudadanos sin tener que recurrir a las comunicaciones de prensa o medios tradicionales, además de ser inmediata. A pesar de esto, se ha comprobado por algunos analistas que la interacción en este tipo de páginas web entre los ciudadanos y los grupos políticos sigue siendo baja. Debido a esto, podríamos decir que estas páginas web realizan una función informadora más que una función comunicadora¹².

⁸Centro de Investigaciones Sociológicas, DEL “Postelectoral elecciones Generales 2016”, *Distribuciones marginales*, 2016, p. 3.

http://www.cis.es/cis/export/sites/default/Archivos/Marginales/3140_3159/3145/es3145mar.pdf

⁹ HELD, D. DEL, *Modelos de democracia*. Madrid, Alianza Editorial, 2007, p. 336.

SUBIRATS, J. DEL, *Los dilemas de una relación inevitable: innovación democrática y tecnologías de la información y de la comunicación* en CAIRO, H: *Democracia digital. Límites y oportunidades*, Madrid, Trotta, 2002, p. 91.

¹⁰ HINOJOSA NAVARRO, G. DEL “Un intento de ciberdemocracia en España: el portal participativo “Decide Madrid” del Ayuntamiento de Madrid”. *Estudios sobre el Mensaje Periodístico*, 2019, vol. 25, no 2, p. 883.

¹¹ LÉVY, P. DEL, *Ciberdemocracia. Ensayo sobre filosofía política*, Barcelona, UOC, 2004, p. 10.

¹² “La información remite simplemente a la transmisión (emisión y recepción) de conocimientos estructurados, mientras que la comunicación consistiría en intercambios de información con objeto de cambiar el comportamiento de los otros” (Weiss citado por, BARTOLI, A. DEL, *Comunicación y Organización. La organización comunicante y la comunicación organizada*, Paidós Ibérica 1992, p. 69).

Otra de las medidas adoptadas, y la que más repercusión tiene a nivel nacional, es el uso de las redes sociales por parte de los dirigentes y demás participantes. No es extraño ver a los políticos detrás de sus perfiles “enzarzarse” con otros compañeros e incluso con otros usuarios que responden a sus mensajes con posturas radicalmente opuestas. También utilizan esta herramienta para hacer propaganda de las nuevas medidas o propuestas, ya que tiene una gran difusión entre todo tipo de público.

La red social por excelencia para este tipo de manifestaciones es Twitter, donde prácticamente todos los representantes cuentan con un perfil y miles de seguidores. Esta tendencia no solo resulta llamativa en España, de hecho, un ejemplo de cómo estas redes sociales influyen en la política es el perfil de Donald Trump, con “tweets” muy controvertidos en los que se pueden ver desde mensajes electoralistas, hasta “advertencias” hacia otros líderes políticos.

1.3.1. Riesgos del uso de las NTIC

Uno de los principales riesgos que derivan de la implementación de las NTIC y, sobre todo, del auge de las redes sociales para este tipo de comunicación propagandística, es el efecto de las denominadas “fake news”¹³.

Aunque siempre han existido relatos sesgados, hasta este momento no se había tenido la capacidad de emitirlos de modo que alcancen audiencias millonarias en cuestión de horas o de pocos días. Además, previamente había que someter el discurso a los canales de distribución establecidos, mientras que, actualmente, una gran parte de las noticias a las que se accede a lo largo del día llega a través de los motores de búsqueda o de los algoritmos de las redes sociales, para los que no influye la veracidad de los datos o la profundidad del estudio.

“En este contexto, la capacidad del lector para diferenciar entre noticias y relatos, entre información y propaganda, entre datos y adoctrinamiento, es fundamental para la preservación de su capacidad para decidir de forma racional”.

¹³ “Una fake new no es necesariamente una mentira, pero ciertamente tampoco es una noticia. Son relatos interesados que pretenden influir en nuestra percepción de la realidad con absoluta falta de respeto por la veracidad de sus contenidos”.

GÓMEZ DE AGREDA, A. DEL, “Falsas noticias, no noticias falsas”, *Telos: Cuadernos de comunicación e innovación*, 2018, p.1.

1.3.2. Conflicto entre las NTIC y la protección de datos

Con la entrada de internet a la vida cotidiana y la rápida difusión de las NTIC, se ha producido una interferencia en la esfera de los derechos fundamentales, principalmente en el referente a la protección de datos de carácter personal, tipificado en el artículo 18 en su apartado 4 de la Constitución Española de 1978 y enunciado como sigue: *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*¹⁴.

Este artículo de la Constitución Española está desarrollado de manera más extensa en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que es el que determina el alcance de la protección. Por otra parte, esta Ley de 1999 queda derogada mediante la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que pretende; en primer lugar, la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos; y en segundo lugar, garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en la Constitución¹⁵.

Además, desde el 25 de mayo de 2018 es directamente aplicable el Reglamento Europeo de Protección de Datos¹⁶. Este Reglamento, respecto de la normativa anterior, amplía los derechos de los ciudadanos, configurándose nuevos derechos de limitación al tratamiento y portabilidad, y ampliándose el contenido del derecho de información en la recogida de los datos personales.

Entre otras cosas, el RGPD establece que es de aplicación al tratamiento de datos personales de ciudadanos que residan en la Unión Europea por parte de encargados no establecidos en la Unión, cuando:

- Las actividades de tratamiento de datos estén relacionadas con la oferta de bienes o servicios a los ciudadanos de la Unión Europea.

¹⁴ Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311, art. 18.

¹⁵ Del Estado, J. DEL, “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”. *Boletín Oficial del Estado*, 294, 2018.

¹⁶ A partir de ahora RGPD

- Cuando se realice el control de su comportamiento, en la medida que este tenga lugar en la unión.

Es decir, aquellas empresas situadas fuera de la Unión que ofrezcan sus servicios o productos a través de internet a los europeos deberán cumplir con el RGPD¹⁷.

Esta injerencia en la esfera personal de los ciudadanos puede variar desde la recolección de datos para un estudio de mercado acerca de los gustos de los consumidores sobre un producto o servicio, hasta el análisis y tratamiento ilícito de estos datos sobre las preferencias políticas de cada individuo para realizar un perfil personalizado y así poder conducir la voluntad de voto hacia algún candidato en concreto, tal y como sucedió con el caso Cambridge Analytica¹⁸.

Redes sociales como Twitter o Facebook son lugares en los que, de manera involuntaria o inconsciente, las personas dejan un rastro de su intimidad al marcar publicaciones como favoritas, los llamados “me gusta”, o simplemente expresar una opinión a lo que la persona cree que es su círculo de “seguidores” o “amigos”, en palabras de estas aplicaciones. En realidad, todas esas huellas son datos de interés sobre la personalidad o las tendencias políticas de cada individuo, por lo que la protección del ciudadano en estos casos ha de verse reforzada y contar con las garantías necesarias para que su tratamiento entre dentro de los márgenes de la legalidad.

A esto nos referiremos de manera más extensa en el capítulo 3 del trabajo.

¹⁷ Agencia Española de Protección de Datos (2019). Protección de Datos: Guía para el Ciudadano. Recuperado de <https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf>

¹⁸ La Comisión Federal de Comercio de Estados Unidos investigó a Facebook en 2018 porque se reveló que a través de un test de personalidad se recolectaron datos de los usuarios que se vendieron a Cambridge Analytica. Estos datos, se cree que pudieron haber sido utilizados para influenciar los resultados de las elecciones de 2016 en Estados Unidos y el referendo del Brexit en Reino Unido también en 2016.

CAPÍTULO 2: RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS POLÍTICOS

En este apartado vamos a desglosar las normativas por territorios dependiendo del alcance, dividiendo en normas jurídicas de rango comunitario, las del Consejo de Europa y aquellas que sean de ámbito nacional. Todas las regulaciones van a aplicarse de forma integrada y coordinada, para así conseguir una protección completa de los datos más sensibles de los ciudadanos frente a sus nuevas formas de obtención.

2.1. Régimen jurídico a nivel comunitario

En primer lugar, la *Carta de los Derechos Fundamentales de la Unión Europea*¹⁹, en su artículo 8, establece la protección de datos de carácter personal, donde toda persona tiene derecho a ser protegido en cuanto a los datos que le conciernan. Tratándose los mismos de modo leal y para fines concretos, contando en todo momento con el consentimiento de la persona afectada y estando éstos sujetos al control de una autoridad independiente. También se reconoce este derecho en el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

Siguiendo la línea temporal, en 2002 el Parlamento Europeo y el Consejo emitieron una *Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*²⁰. Esta Directiva se adoptó en un momento en el que Internet estaba revolucionando las estructuras tradicionales de comunicación, donde los nuevos servicios de comunicaciones electrónicas disponibles al público a través de internet ofrecían nuevas posibilidades para los usuarios, pero también entrañaban nuevos riesgos que ponían en peligro sus datos personales y su intimidad. La Directiva sienta las normas sobre almacenamiento de información y la obtención del acceso a la información ya almacenada, como las “cookies”, que puedan utilizarse para rastrear el comportamiento en línea de un usuario, ya sea en un teléfono inteligente o en un ordenador.

¹⁹ DOUE. DEL, “Carta de los Derechos Fundamentales de la Unión Europea”, 2010.

²⁰ Europea, U. DEL, “Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales ya la protección de la intimidad en el sector de las comunicaciones electrónicas”, *Diario Oficial de las Comunidades Europeas L*, 201, 2002.

Al igual que la ya derogada *Directiva 95/49/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, la presente regulación no interfiere en la capacidad de los Estados miembros para interceptar legalmente comunicaciones electrónicas cuando sea necesario con el objetivo de proteger la seguridad pública, la defensa, la seguridad del Estado y la aplicación del Derecho Penal, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales.

Como regulación fundamental en el marco europeo comunitario y también de aplicación directa en los Estados, nos encontramos ante el *Reglamento (UE) General de Protección de Datos 2016/679*²¹, que entró en vigor el 25 de mayo de 2016, aunque su plena aplicación no se hizo efectiva hasta el 25 de mayo de 2018. Si la Directiva 2002/58/CE se adoptó en un momento en el que Internet estaba en auge, este Reglamento podemos afirmar que se ha adoptado en el momento de máximo esplendor de las redes sociales. Actualmente los ciudadanos comparten más datos personales, ya sea a través de teléfonos inteligentes, redes sociales, banca por internet o transferencias globales, y las empresas disponen de más capacidad para recoger y gestionar esos datos²².

Es por ello que se hace necesaria una regulación adecuada para la protección de datos en los países pertenecientes a la UE, que esté adaptada a la globalización y al desarrollo tecnológico²³, a pesar de que éste siempre irá más rápido que el desarrollo legislativo.

Con respecto a los datos personales sobre las opiniones políticas, el considerando 56 del mencionado Reglamento supone una excepción al artículo 9 de la mencionada ley²⁴, permitiendo su recopilación y tratamiento por razones de interés público, siempre que se ofrezcan las garantías adecuadas. Esto ha sido interpretado por algunos diputados

²¹ Europea, U. DEL, “Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 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)”. *Diario oficial de la Unión Europea*, 4. 2016.

²² REIGADA, A. T. DEL, “Las redes sociales a la luz de la propuesta de Reglamento general de protección de datos personales: Parte uno”, *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, (15), 2012, p. 61-75.

²³ MARTÍNEZ-MARTÍNEZ, D. F. DEL, “Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones”, *El profesional de la información*, 27(1), 2018, p.185-194.

²⁴ En virtud del artículo 9 RGPD queda prohibido el tratamiento de datos personales que revelen, entre otras cosas, las opiniones políticas.

socialistas como un precedente vinculante del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General ya declarado inconstitucional por el Tribunal Constitucional. Debido a esto, existe la necesidad de regular la presencia tecnológica en las campañas electorales y proteger los datos a través de las normativas en el contexto electoral²⁵.

“El RGPD armoniza conceptos tales como el consentimiento, refuerza los derechos de la persona a ser informada sobre el tratamiento de sus datos, precisa las condiciones en las que pueden transmitirse a otros datos personales, introduce normas sobre violaciones de los datos personales y establece un mecanismo de cooperación entre las autoridades en materia de protección de datos en casos transfronterizos” tal y como indica el *Documento de Orientación para unas elecciones libres y limpias*, emitido por la Comisión²⁶.

En un proceso electoral intervienen distintos agentes además de los partidos políticos, y todos ellos están sometidos a los requisitos contenidos en el RGPD, siempre que traten datos personales o utilicen perfiles de los votantes. Para asegurar que la elaboración de perfiles cumple con la exigencia de ser comunicado a los sujetos objeto del mismo si tiene consecuencias en sus derechos de participación política, se crearon las Directrices del Grupo de Trabajo del Artículo 29²⁷, sobre *Decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*²⁸.

El RGPD introduce nuevas disposiciones para afrontar los riesgos derivados de la elaboración de perfiles, como la segregación social o una discriminación injustificada y, la tarea del GT29²⁹ es aclarar dichas disposiciones asegurándose de la aplicación de las directrices.

²⁵ ADSUARA VARELA, B. /MARTÍNEZ MARTÍNEZ, R. DEL, “Debate sobre el nuevo artículo 58 bis de la LOREG”, La Ley Privacidad, nº1, *Diario la Ley (online)*, 2019.

²⁶ Europea, C. DEL, “Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral, COM (2018) 638 final”, *Diario Oficial de la Unión Europea*, 2018.

²⁷ A partir de ahora GT29

²⁸ Grupo de Trabajo sobre Protección de Datos del artículo 29. “Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679”. WP25rev.01, 17/ES, 2018.

²⁹ Este Grupo de Trabajo se creó en virtud de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos e intimidad. Cesó su actividad en mayo de 2018 con la entrada en aplicación del RGPD.

En 2018 el Supervisor Europeo de Protección de Datos³⁰ elaboró un *Dictamen sobre la manipulación en línea y los datos personales* debido al gran debate público que se estaba produciendo y que aún continúa siendo un gran foco de controversia, sobre los efectos que tiene el inmenso y complejo ecosistema de información digital para la economía política, es decir, cómo interactúa el entorno político con la economía. Además, todos los pasos en Internet que van dando las personas, sus acciones y gustos se registran automáticamente dejando un rastro de “migas de pan digitales”³¹ que permiten predecir su personalidad y comportamiento, para así realizar un perfilado de los mismos. Para segmentar y personalizar los mensajes que se envían a los ciudadanos hacen falta datos, y la mayoría de los anunciantes no saben cómo se toman este tipo de decisiones y la mayoría de los ciudadanos no saben cómo se utilizan dichos datos³².

Es por esto que la finalidad del Dictamen es tratar de puntualizar los problemas principales que se están sufriendo y proponer medidas tanto éticas como técnicas para que los ciudadanos tengan control sobre los datos personales que les conciernen, y la rendición de cuentas en la aplicación de la ley. A pesar de que este Dictamen no es vinculante, sus recomendaciones, entre ellas que los reguladores deben cooperar entre sectores o la obligación de hacer cumplir y completar las reglas de protección de datos, son de gran utilidad para la buena aplicación de la normativa europea, concretamente el RGPD.

Con la proximidad de las elecciones al Parlamento Europeo de mayo de 2019, el SEPD en diciembre de 2018, elaboró un segundo *Dictamen sobre el paquete de la Comisión relativo a unas elecciones europeas libres y justas*³³. En éste, el SEPD reconoce la comunicación política como un factor esencial en la participación de los ciudadanos, las fuerzas políticas y los candidatos en la vida democrática y para el derecho fundamental a la libertad de expresión. Sin embargo, considera que, para una mayor claridad, podría haberse incluido una referencia al tratamiento de datos personales por parte del

³⁰ A partir de ahora SEPD

³¹ Supervisor Europeo de Protección de Datos. DEL, “La manipulación en línea y los datos personales, Dictamen 3/2018”, *Europe Publication*, 2018. Recuperado de:

https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

³² Supervisor Europeo de Protección de Datos. DEL, “Resumen del Dictamen del SEPD sobre la manipulación en línea y los datos personales”, *Diario Oficial de la Unión Europea C 233/8*, 2018.

³³ Supervisor Europeo de Protección de Datos. DEL, “El paquete de la Comisión relativo a unas elecciones europeas libres y justas, Dictamen 10/2018”, *Europe Publication*, 2018. Recuperado de: https://edps.europa.eu/sites/edp/files/publication/18-12-18_opinion_on_election_package_en.pdf

Parlamento Europeo, de la Autoridad y el Comité para afirmar su inclusión dentro del ámbito del Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de estos datos³⁴.

El paquete de la Comisión mencionado por el SEPD hace referencia a un conjunto de documentos emitidos en el ámbito de las elecciones al Parlamento Europeo, compuesto por una *Recomendación con vistas a reforzar el carácter europeo y el desarrollo eficiente de las elecciones de 2019 al Parlamento Europeo*, en la que se incluían propuestas tales como involucrar a los ciudadanos europeos en debates sobre cuestiones europeas antes de las elecciones al Parlamento Europeo. También, debido a los riesgos que suponen para los procesos electorales los ciberataques y la desinformación, se propone fomentar el intercambio de experiencias entre los Estados miembros sobre las cuestiones conexas³⁵.

Este paquete incluía también una *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones para garantizar unas elecciones europeas libres y justas*, de septiembre de 2018, donde se pone de manifiesto la necesidad de proteger la democracia en la Unión frente a los riesgos de manipulación del proceso electoral o ataques a los sistemas de información, ya sea mediante el uso indebido de datos personales o de prácticas opacas³⁶.

El mismo día se emitió también un documento con *Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral*, que buscaba aportar claridad a la aplicación del RGPD ya que la primera vez que se aplicaban estas normas en el contexto electoral era en las elecciones al Parlamento Europeo. En este contexto, se debían remarcar las obligaciones en materia de protección de datos relevantes a los agentes implicados en el proceso electoral, como

³⁴ SEPD, DEL, “Resumen del Dictamen del SEPD sobre el paquete de la Comisión relativo a unas elecciones europeas libres y justas”, *Diario Oficial de la Unión Europea* C 47/8, 2018.

³⁵ Europea, C. DEL, “Recomendación (UE) 2018/234 con vistas a reforzar el carácter europeo y el desarrollo eficiente de las elecciones de 2019 al Parlamento Europeo L45/40”, *Diario Oficial de la Unión Europea*, 2018.

³⁶ Europea, C. DEL, “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM (2018) 637 final”, *Diario Oficial de la Unión Europea*, 2018.

son las autoridades electorales nacionales, partidos políticos, intermediarios y analistas de datos, plataformas de redes sociales y redes de publicidad en línea³⁷.

Y, por último, a este paquete se incorporó una propuesta de Reglamento que terminó por materializarse en el *Reglamento del Parlamento Europeo y del Consejo en lo que respecta a un procedimiento de verificación relativo a las infracciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo*, aprobado en 2019. En él se incluye un procedimiento de verificación para comprobar si algún partido político europeo ha influido o ha intentado influir en el resultado de las elecciones, aprovechándose de una infracción de las normas aplicables en materia de protección de datos personales y, de ser así, imponerle una sanción proporcionada y disuasoria del sistema de sanciones efectivo establecido en el Reglamento n.º 1141/2014³⁸.

Algunas empresas como Facebook, Google, Microsoft o Twitter se adhirieron en 2018 al *Código de buenas prácticas en materia de desinformación de la Unión Europea*, siendo así vinculante tanto para éstas como para las demás signatarias. Este Código se aprobó teniendo en cuenta la Comunicación de la Comisión Europea llamada “La lucha contra la desinformación en línea: un enfoque europeo”, el informe del Grupo de expertos de alto nivel, las Conclusiones del Consejo del 28 de junio de 2018 y las diversas iniciativas que estaban teniendo lugar en toda Europa para abordar los retos planteados por la difusión de la desinformación³⁹. Entre sus objetivos se encontraba garantizar la transparencia de la publicidad política relativa a cuestiones de interés general, entre otras cosas, permitiendo que los usuarios sepan por qué han sido objetivo de un determinado anuncio publicitario y mejorar el análisis de la colocación de los anuncios publicitarios para reducir los ingresos de los proveedores de desinformación.

³⁷ Europea, C. DEL, “Orientaciones de la Comisión..., op., cit.

³⁸ Europeo, P. y Consejo, DEL, “Reglamento (UE, Euratom) 2019/493 por el que se modifica el Reglamento (UE, Euratom) n.º 1141/2014 en lo que respecta a un procedimiento de verificación relativo a las infracciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo L85 I/7”, *Diario Oficial de la Unión Europea*, 2019.

³⁹ Europea, C. DEL, “Código de buenas prácticas en materia de desinformación”, *Policies, information and services*, 2018. Recuperado de:
<https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>

A pesar de que, en comparación con octubre de 2018, los signatarios presentan una mayor transparencia, el alcance de las acciones emprendidas por cada plataforma para cumplir sus compromisos varía significativamente⁴⁰.

En el período entre los dos Dictámenes del SEPD, se aprobó el *Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos*⁴¹. Este Reglamento se asienta sobre los pilares del Reglamento 2016/679 y comparte su misma estructura, enfatizando la necesidad de proteger a las personas cuyos datos son tratados por las instituciones y organismos de la Unión en cualquier contexto. Sin embargo, no regula el tratamiento de datos personales relativos a personas jurídicas⁴².

Pone el foco en el consentimiento del interesado, al igual que el RGPD, estableciendo que solo será válido si es prestado a través de un acto afirmativo claro, como puede ser una declaración, tanto verbal como escrita, o una declaración electrónica. Fundamentalmente, este Reglamento pretende garantizar la eficacia del RGPD en relación con los tratamientos de datos personales que llevan a cabo los organismos de la Unión Europea⁴³.

2.2. Régimen jurídico del Consejo de Europa

En primer lugar, como documento con más antigüedad a la par que mayor importancia debido a su trascendencia global, nos encontramos con el *Convenio Europeo de Derechos Humanos*⁴⁴, adoptado por el Consejo de Europa por primera vez en 1950 y que entró en

⁴⁰ Europea, C. DEL, “El código de buenas prácticas contra la desinformación cumple un año: las plataformas en línea presentan informes de autoevaluación, STATEMENT/19/6166”, *Declaración, Zona de Prensa*, 2019.

Recuperado de: https://ec.europa.eu/commission/presscorner/detail/es/STATEMENT_19_6166

⁴¹ Europeo, P. y Consejo, DEL, “Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE”, *Diario Oficial de la Unión Europea*, 2018.

⁴² ABAJO, J. DEL, “2018 despidió el año con un nuevo reglamento en materia de protección de datos”, *Derecho digital e Innovación Tecnológica H&A*, 2018.

⁴³ MAHAMUT, R. G., & CORDERO, J. V. DEL, “La protección de los datos personales de los solicitantes de protección internacional en el (nuevo) Sistema Europeo Común de Asilo: grandes desafíos y graves deficiencias”. *Teoría y realidad constitucional*, (44), 2019, p. 237-270.

⁴⁴ de Europa, C. DEL, “Convenio Europeo de Derechos Humanos, Tribunal Europeo de Derechos Humanos”, *F-67075 Strasbourg cedex*.

vigor en 1953. A partir de ahí ha sufrido distintas modificaciones, siendo la última en 2018 a través de las disposiciones del Protocolo nº16, el cual España de momento, no tiene pensado firmar⁴⁵. En su artículo tres dentro del Protocolo Adicional se establece el Derecho a unas elecciones libres, en condiciones que garanticen la libre expresión de la opinión del pueblo en la elección del cuerpo legislativo, esto es, sin interferencias de Agentes externos que participen en el proceso electoral.

Más adelante, en 2010, el Consejo de Ministros de Justicia del Consejo de Europa adoptó la *Resolución n.º 3 sobre la Protección de Datos y la Privacidad en el tercer milenio*. En esta se comprometen a apoyar la modernización del Convenio 108⁴⁶ con el objetivo de encontrar soluciones apropiadas a los nuevos retos planteados por la tecnología y la globalización de la información. Así se podrá garantizar la protección efectiva de los derechos humanos y las libertades fundamentales, además del ejercicio de esos derechos, particularmente el derecho a respetar la vida privada mientras se procesan los datos personales, y resolver los problemas de transparencia, brechas de seguridad y jurisdicción. También se comprometieron a impulsar la firma del Convenio 108 por aquellos países que aún no lo habían hecho. Y, por último, pedirle al Secretario General del Consejo de Europa presentar un informe sobre los pasos que se van dando para darle efectividad a esta Resolución con motivo de su próxima Conferencia⁴⁷.

También en el año 2010 se adoptó la *Recomendación del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles*. En esta Recomendación se hace mención a los principios generales que rigen la protección de datos, las condiciones para la recopilación y el tratamiento de datos de carácter personal en el contexto de la creación de perfiles con relación a la legalidad, la calidad de los datos, los datos delicados, la información que se recopila o los derechos de las

⁴⁵De España, G. Ministerio de Justicia, DEL, “Entrada en vigor del Protocolo nº16 al Convenio Europeo de Derechos Humanos”, *Área Internacional Portal Ministerio de Justicia*, 2019. Recuperado de: https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428869010?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DEntrada_en_vigor_del_Protocolo_n_16_al_Convenio_.PDF&blobheadervalue2=Docs_TEDH_Tribunal

⁴⁶ *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*

⁴⁷ Of Europe, C. DEL, “Resolution N.º 3 on data protection and privacy in the third millennium, MJU-30 RESOL,3E”, *30th Council of Europe Conference of Ministers of Justice*, 2010.

personas interesadas. Con respecto a los datos delicados, como son las opiniones políticas, se establece que su recopilación y tratamiento en el contexto de la creación de perfiles está prohibido salvo que sean necesarios para fines legítimos y específicos, siempre que la persona haya dado su consentimiento con la previsión de unas garantías adecuadas⁴⁸.

El Consejo de Europa emitió en 2017 unas *Directrices sobre la protección de las personas con respecto al procesamiento de datos personales en el mundo del Big Data*, con el objetivo de proveer de un marco general a los partidos políticos para aplicar las medidas y políticas adecuadas con la intención de hacer efectivos los principios y provisiones de la Convención 108 en el contexto del Big Data. En este documento se proponen nueve directrices y principios, entre los que se incluyen desarrollar y proporcionar medidas apropiadas, como soluciones “por diseño” y soluciones “por defecto”, para mitigar los riesgos⁴⁹.

Todos los documentos emitidos por el Consejo de Europa y por otros organismos, en mayor o en menor medida, hacen referencia al *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, denominado Convenio 108 y adoptado en 1981 en Estrasburgo, ratificado en 1984 por España⁵⁰.

Este Convenio es el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos, cuyo objetivo es proteger el derecho a la vida privada, reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. Además, fue una de las fuentes de inspiración para la elaboración del acervo de la UE en este ámbito y, obliga a las Partes a incorporar a su ordenamiento jurídico interno las disposiciones necesarias para garantizar el respeto de los derechos humanos de todas las personas en lo que respecta al tratamiento de sus

⁴⁸ De Europa, C. DEL, “Recomendación CM/Rec (2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles”, *Portal del Consejo de Europa*, 2010.

⁴⁹ Of Europe, C. DEL, “Convention for the protection of individuals with regard to automatic processing of personal data”, *Directorate General of human Rights and Rule of Law*, 2017.

⁵⁰ Del Estado, J. DEL, “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981”, *Boletín Oficial del Estado*, 1984.

datos personales⁵¹. En 2018 se acumulaban un total de 51 Estados que habían ratificado el Convenio, incluida la totalidad de los, en ese momento, 28 Estados miembros de la UE.

Se han ido sucediendo distintos documentos que complementan este Convenio con el objetivo de adaptarlo a los distintos momentos sociales, como en 2001 con el *Instrumento de Ratificación del Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos*. En él se incluyen novedades como la posibilidad de las Autoridades destinadas al cumplimiento del Convenio para poder investigar e intervenir, así como llamar la atención a las Autoridades nacionales que no cumplan con las disposiciones de derecho interno que dan efecto a los principios del Convenio⁵².

La última propuesta de modificación ha sido en 2018, en lo que se refiere a la Decisión por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio 108, de ahora en adelante, “Protocolo modificativo”. Este Convenio modernizado (por el Protocolo modificativo) incluye una novedad muy importante y es que tendrá un ámbito de aplicación uniforme para todas las Partes del Convenio, sin la posibilidad de excluir completamente de su ámbito de aplicación determinados sectores, como es el caso en el Convenio 108 vigente. Así, todo tipo de tratamiento de datos estará protegido bajo la jurisdicción de las Partes, tanto en el sector público como en el privado⁵³. También se reforzará la protección de categorías especiales de datos y se ampliarán dichas categorías, ofreciendo salvaguardias adicionales para las personas cuyos datos personales sean objeto de tratamiento a la vez que se reforzarán sus derechos⁵⁴.

⁵¹ Europea, C. DEL, “Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal” COM 451 final, *Diario Oficial de la Unión Europea*, 2018.

⁵² Del Estado, J. DEL, “Instrumento de Ratificación del Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001”, *Boletín Oficial del Estado*, 2001.

⁵³ Of Europe, C. DEL, “The modernised Convention 108: novelties in a nutshell”, *Diario Oficial de la Unión Europea*, 2018.

⁵⁴ GEORGES, M & KORFF, D. DEL “El Manual del Delegado de Protección de Datos. Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del RGPD”, *Agencia Española de Protección de Datos*, 2019.

Como último documento a destacar, encontramos el *Informe de la Comisión de Venecia sobre Tecnologías Digitales y Elecciones*, que hace un repaso de todos los riesgos y escenarios que se han ido subrayando a lo largo de este apartado y, concluye con que la posibilidad de acceder a unas elecciones democráticas, desde los inicios de la democracia, es imposible si no se respetan los derechos humanos, fundamentalmente la libertad de expresión y prensa, y la libertad de reunión y asociación con fines políticos, incluyendo la creación de partidos políticos. Incide en la difícil relación entre la democracia y las nuevas tecnologías, debido a que en los últimos años las redes sociales se han convertido en la plataforma principal de interacción política y, por ende, los niveles de “fake news” o desinformación han ido en aumento. Es por esto que hace referencia a la necesidad de una legislación eficazmente implementada sobre el proceso electoral y los mecanismos ordinarios de justicia⁵⁵.

2.3. Régimen jurídico a nivel nacional

Como primera y principal normativa a tener en cuenta encontramos la *Ley Orgánica 5/1985 del Régimen Electoral General*,⁵⁶ que se encarga de regular los procesos electorales, la campaña electoral, la entrega de la copia del censo electoral a los partidos políticos, la propaganda electoral, o del uso de los medios tecnológicos por parte de los partidos políticos⁵⁷.

Esta ley dispone que los datos personales de los electores que sean necesarios para su inscripción en el censo, así como los de las listas y copias del censo, se regularán por real decreto. Además, los representantes de cada candidatura podrán obtener una copia del censo del distrito correspondiente, en soporte informático, que podrá ser utilizado exclusivamente para los fines previstos en la ley⁵⁸.

⁵⁵ Europea, C. Para la democracia a través del Derecho. DEL “Informe conjunto de la Comisión de Venecia y de la Dirección de la Sociedad de la Información y lucha contra la delincuencia de la Dirección General de Derechos Humanos y Estado de Derecho sobre Tecnologías Digitales y Elecciones”, *CDL-AD (2019)016, Opinion No. 925/2018*, 2019. Recuperado de:

[http://www.cepc.gob.es/docs/default-source/comisionveneciadoc/cdl-ad\(2019\)016-e.pdf?sfvrsn=0](http://www.cepc.gob.es/docs/default-source/comisionveneciadoc/cdl-ad(2019)016-e.pdf?sfvrsn=0)

⁵⁶ Del Estado, J. DEL, “Ley Orgánica 5/1985, de 10 de junio, del Régimen Electoral General”, *Boletín Oficial del Estado*, 1985.

⁵⁷ GARCÍA MAHAMUT, R. DEL “Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español”, *Teoría y Realidad Constitucional*, nº35, 2015, p. 309-338.

⁵⁸ PRODAT. DEL, “Boletín nº2 Febrero 2009”, *Boletín PRODAT*, 2009. Recuperado de: <https://www.prodat.es/boletin/febrero2009/legislacion.html>

El artículo cincuenta y tres de la mencionada ley establece la prohibición de difundir propaganda electoral y la realización de cualquier acto de campaña electoral una vez que esta haya terminado legalmente. Sin embargo, los partidos políticos utilizan los avances tecnológicos de forma permanente en su función de formación de la opinión pública.

El contenido de estas listas y las copias del censo se regula en otra normativa, como es el *Real Decreto 1799/2003*, del que cabe remarcar que no recoge el dato del correo electrónico ni el número de teléfono móvil, por lo que el envío de propaganda electoral a una dirección de correo electrónico requiere, en todo caso, el consentimiento del elector que lo haya facilitado.

Hasta la aprobación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales⁵⁹, fue la Junta Electoral Central⁶⁰ quien se encargó de colmar las lagunas que surgieron debido a las nuevas tecnologías de la información y de comunicación electrónica. La *Instrucción 4/2007 de la Junta Electoral Central sobre la utilización de las nuevas tecnologías de la información y de la comunicación electrónicas como instrumento de propaganda electoral*, y la *Instrucción 3/2011 de la JEC sobre la interpretación de la prohibición de realización de campaña electoral incluida en el artículo 53 de la LOREG*, vienen a plasmar la interpretación de la JEC en su Acuerdo de 1991. Se establece que el envío de propaganda electoral a través de las nuevas tecnologías de información y de las comunicaciones electrónicas no es un acto prohibido por la normativa electoral⁶¹, siempre que no se solicite el voto. Sin embargo, estas comunicaciones se someten a las disposiciones de la LOREG en cuanto a las limitaciones en materia de campaña electoral o propaganda⁶². Queda claro entonces que el spam político no se encuentra prohibido en campaña electoral porque no se considera spam⁶³, si no simplemente una alternativa de comunicación adaptada al nuevo contexto social.

⁵⁹ A partir de ahora LOPDGDD

⁶⁰ A partir de ahora JEC

⁶¹ JEC, DEL, “Instrucción 3/2011 sobre interpretación de la prohibición de realización de campaña electoral incluida en el artículo 53 de la Ley Orgánica del Régimen Electoral General”, *Boletín Oficial del Estado*, 2011.

⁶² JEC, DEL, “Instrucción 4/2007 sobre la utilización de las nuevas tecnologías de la información y de la comunicación electrónicas como instrumento de propaganda electoral”, *Boletín Oficial del Estado*, 2007.

⁶³ Esta es una de las novedades introducidas en la LOREG tras la aprobación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Antes de esto, las comunicaciones electrónicas podían ser consideradas como spam, lo cual está prohibido por el artículo 21 de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.

Con la aprobación de la LOPDGDD quedan derogadas la *Ley Orgánica de Protección de Datos 15/1999 de protección de datos de carácter personal* salvo sus artículos 22, 23 y 24, y también, según su Disposición Derogatoria única “quedan derogadas cuantas disposiciones de igual o inferior rango se contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica”⁶⁴. De este precepto se deduce que el *Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999* no está derogado en su totalidad, sino únicamente las disposiciones que cumplan con esta descripción. Por lo tanto, las medidas de seguridad establecidas en este Real Decreto se han de tener en cuenta, y se deben mantener y revisar en el marco de los procesos de análisis de riesgos establecidos por el RGPD⁶⁵.

Según lo dispuesto en el artículo 1 de la LOPDGDD, esta norma jurídica tiene por objeto adaptar el ordenamiento jurídico español al RGPD y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución Española se ejercerá con arreglo a lo establecido en el Reglamento 2016/679 y en la LOPDGDD. Además, se pretenden garantizar los derechos digitales de la ciudadanía conforme a lo establecido en el artículo 18.4 de la Constitución⁶⁶.

En esta nueva regulación se introducen muchas novedades, entre ellas la determinación de la edad para el consentimiento lícito de los menores de edad, que se marca en 14 años según lo dispuesto en el artículo 7. En el artículo 8 del RGPD, que regula las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, se indica que el tratamiento de los datos personales de un niño se considera lícito cuando tenga mínimo 16 años, aunque contempla que los Estados miembros puedan establecer por ley una edad inferior, siempre que no sea inferior a 13 años⁶⁷.

⁶⁴ Del Estado, J. DEL, “Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales”, *Boletín Oficial del Estado*, 2018.

⁶⁵ Ministerio de Justicia, DEL, “Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal”, *Boletín Oficial del Estado*, 2008.

⁶⁶ Del Estado, J. DEL, “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”. *Boletín Oficial del Estado*, 294, 2018

⁶⁷ GÓMEZ, R. M. DEL, “Principales novedades de la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (16), 2018, p. 201-246.

Conforme a la anterior previsión, en la LOPDGDD se ha mantenido la edad de 14 años que se contemplaba en la normativa nacional, para que el tratamiento de los datos personales de un menor pueda fundarse en su consentimiento.

Una de las principales novedades de la norma es el reconocimiento y garantía de nuevos derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución Española, entre los que se encuentran el derecho a la seguridad digital, el derecho al olvido en búsquedas de internet o el derecho al olvido en redes sociales y servicios equivalentes.

La modificación de la Ley Orgánica del Régimen Electoral General, con la inclusión del artículo 58 bis, supuso la apertura de un acalorado debate sobre la vulneración de un derecho fundamental como es el derecho a la protección de datos del artículo 18.4 de la Constitución Española. Este controvertido artículo, en su apartado primero, permitía la recopilación de datos personales relativos a las opiniones políticas de las personas por parte de los partidos políticos en el marco de sus actividades electorales, siempre que se motive en un interés público y con unas garantías adecuadas.

Ante la deficiente redacción del citado artículo de la LOREG, la Agencia Española de Protección de Datos⁶⁸ emitió el *Informe jurídico 210070/2018 sobre tratamiento de datos de opiniones políticas por todos los partidos políticos*, que se complementó con la *Circular 1/2019*⁶⁹. Ambos documentos especificaban, entre otros aspectos, la excepcionalidad de la posibilidad atribuida a los partidos políticos; la necesidad de que la finalidad sea clara y determinada para legitimar el tratamiento; la obligatoriedad de determinar los sujetos que pueden realizar los tratamientos; y la necesidad de concretar los datos a ser tratados, así como los tratamientos y el momento en el que pueden producirse⁷⁰. Dicho artículo ha sido declarado inconstitucional por la Sentencia del Tribunal Constitucional 76/2019, que estudiaremos en profundidad en el siguiente apartado.

⁶⁸ A partir de ahora AEPD

⁶⁹ AEPD, DEL, “Circular 1/2019, de 7 de marzo, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la LOREG”, *Boletín Oficial del Estado*, 2019.

⁷⁰ LÓPEZ MARTÍNEZ, J. DEL, “Partidos políticos y datos personales de los ciudadanos. ¿Qué pueden usar y para qué?”, *SEPIN*, 2019.

CAPÍTULO 3: ANÁLISIS DE LA SENTENCIA 76/2019 DEL TRIBUNAL CONSTITUCIONAL

Como ya se ha mencionado a lo largo del trabajo, la Ley Orgánica de protección de datos personales y garantía de los derechos digitales introdujo, a través de su disposición final tercera apartado segundo, el artículo 58 bis de la Ley Orgánica del Régimen Electoral General, frente al cual se interpuso un recurso de inconstitucionalidad sobre su apartado primero.

La redacción del artículo establecía lo siguiente:

Artículo 58 bis. Utilización de medios tecnológicos y datos personales en las actividades electorales⁷¹.

- 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 personas obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.*
- 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.*
- 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.*
- 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.*

A pesar de que el grupo socialista presentó la enmienda motivándola en “Adecuar el Reglamento a las especificidades nacionales y establecer salvaguardias para impedir

⁷¹ AEPD, DEL, “Circular 1/2019, de 7 de marzo, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la LOREG”, *Boletín Oficial del Estado*, 2019.

casos como el que vincula a Cambridge Analytica con el uso ilícito de datos de cincuenta millones de usuarios de Facebook para mercadotecnia electoral”⁷², rápido generó un gran descontento entre los ciudadanos y diversas Asociaciones⁷³, que instaron al Defensor del Pueblo a presentar un recurso de inconstitucionalidad.

El recurso se presentó el 5 de marzo de 2019 fundamentándose en tres argumentos principalmente: (i) que la disposición no reflejaba una finalidad determinada que justificara el tratamiento realizado, más allá de la genérica mención al “interés público”; (ii) que el artículo no establecía ni las condiciones, requisitos o restricciones que permitían el tratamiento de los datos; y (iii) que el texto enjuiciado no establecía las garantías adecuadas para proteger los derechos derivados del tratamiento realizado⁷⁴.

Por otro lado, el Abogado del Estado en su escrito de alegaciones solicitó que se desestimara en su integridad el recurso interpuesto por el Defensor del Pueblo argumentando que, de no existir vulneración a la seguridad jurídica, ya que el artículo 58 bis) 1. LOREG respetaba el contenido esencial del derecho a la protección de datos y establecía las garantías adecuadas, decaerían las alegaciones sobre el resto de supuestas vulneraciones de derechos fundamentales. Además, considera lógico que, si tanto el RGPD como la LOPDGDD recogen las garantías adecuadas a las que se refiere la LOREG, no es necesario su desarrollo en el apartado impugnado puesto que ya se encuentran perfectamente previstas.

El Tribunal Constitucional⁷⁵ en sus fundamentos jurídicos comienza identificando el núcleo de la controversia, ya que tal y como presenta el abogado del Estado existe una impugnación central, de las que las demás son complementarias. Sin embargo, dicha impugnación central no es la defendida por el abogado del Estado relativa a la vulneración del principio de seguridad jurídica del artículo 9.3 CE, sino la que se refiere al artículo 18.4 CE en conexión con el art. 53.1 CE, donde se reconoce el contenido esencial del

⁷² De los Diputados, C. DEL, “Enmiendas e Índice de enmiendas al Articulado. 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, núm. 13.2”, *Boletín Oficial de las Cortes Generales*, 2018, p. 209. Recuperado de:

http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-2.PDF

⁷³ Asociación de Internautas (AI), Asociación de Usuarios de Internet (AUI), Plataforma en Defensa de la Libertad de Información (PDLI), Asociación de Expertos Nacionales de la Abogacía Digital (ENATIC), e ISACA Capítulo Madrid.

⁷⁴ STS 76/2019, de 22 de mayo

⁷⁵ A partir de ahora TC

derecho a la protección de datos personales. Es por esto que nuestro Tribunal analiza en primer lugar el contenido esencial del derecho a la protección de datos bajo la condición de que éste mismo puede limitarse, para después analizar dicha limitación, que ha de interpretarse de forma restrictiva, bajo la amenaza de generar indeterminación e incertidumbre, inseguridad jurídica, permitiendo que la aplicación de la norma y la determinación de sus límites quede a “la voluntad de quien ha de aplicarla” y dotando de una más fácil intromisión en el contenido esencial del derecho, alterándolo⁷⁶.

Analizaremos los tres argumentos principales en los que se fundamenta el recurso del Defensor del Pueblo de manera individualizada.

3.1. Fin legítimo

Cualquier tratamiento de datos personales ha de tener una base que lo legitime. Estas bases se establecen tanto el RGPD como en la LOPDGDD, al mismo tiempo que indican que la finalidad perseguida ha de ser determinada y legítima, y también se establecen los principios del tratamiento de datos personales⁷⁷.

En el caso de la recopilación de datos por parte de los partidos políticos, conocer la finalidad es esencial, ya que además de tratarse de datos de carácter especial, requieren el consentimiento del titular, evitando así el riesgo de discrecionalidad y arbitrariedad. Es por eso que, teniendo una finalidad determinada, si las plataformas o servidores *on line* recogen datos con fines comerciales, éstos no podrán ser tratados más tarde en el contexto electoral. “Salvo que las fundaciones y los partidos políticos actúen con diligencia debida y comprueben que los datos han sido obtenidos legalmente, no podrán utilizar este tipo de datos obtenidos de un tercero” ⁷⁸.

En la STC 76/2019, el Tribunal Constitucional considera que la disposición legal impugnada no especifica el interés público esencial que fundamenta la restricción del derecho fundamental, es decir, no especifica la finalidad que legitima a los partidos políticos a obtener las opiniones políticas de los ciudadanos. Añade que la invocación

⁷⁶ RAMIRO ARENAS, M. DEL, “Partidos políticos, opiniones políticas e Internet: la lesión del derecho a la protección de datos personales”. *Teoría y realidad constitucional*, (44), 2019, 341-372.

⁷⁷ El artículo 5.1.b) del RGPD hace referencia al principio de “limitación de la finalidad”

⁷⁸ Extracto perteneciente al Documento de Orientación de la Comisión Europea sobre Elecciones Libres y Limpas, 2018, que se menciona en la página 12 de este trabajo.

genérica de un “interés público” – como dice la LOREG – no puede ser la base de la legitimidad para restringir el derecho fundamental a la protección de datos personales, ya que supondría trasladar a los partidos políticos la posibilidad de establecer los límites y la regulación de un derecho fundamental, tarea que legalmente solo le compete al legislador. Al no poderse identificar con precisión la finalidad del tratamiento de datos, tampoco se podrá juzgar la proporcionalidad de la medida ni el carácter constitucionalmente legítimo de esa finalidad.

Por otro lado, el Tribunal también rechaza el argumento defendido el Abogado del Estado sobre la protección del funcionamiento del sistema democrático, ya que genera demasiada incertidumbre y puede devenir en un “razonamiento circular”⁷⁹.

3.2. Condiciones determinadas

No solo es esencial que el tratamiento de datos tenga una finalidad determinada, sino que todos los aspectos que envuelven dicho tratamiento, y sobre todo cuando se trata de categorías especiales de datos, han de estar concretados, desde quién es el responsable del tratamiento hasta las circunstancias en las que los mismos pueden producirse, como así lo exige el principio de transparencia de los datos⁸⁰.

Teniendo esto en cuenta, además de especificar el interés público que legitime el tratamiento de las opiniones políticas de los ciudadanos por parte de los partidos políticos, el TC analiza el segundo criterio de inconstitucionalidad del art. 58. bis).¹ LOREG, basado en que dicho precepto no establece ni el alcance ni el contenido de los tratamientos de datos que autoriza, ni respecto de los datos tratados, ni respecto de las operaciones realizadas con los mismos, sino que se refiere de manera genérica a una recopilación, pero no concreta si en los tratamientos permitidos las opiniones políticas podrán ser comunicadas o transferidas a terceros.

El problema de la recolección de datos en el entorno on line, es que resulta muy complicado identificar los datos referentes a opiniones políticas y aquellos que no lo son y, por tanto, los datos que pueden ser recopilados, lo que provoca que se puedan recoger más datos de los necesarios o incluso datos inadecuados para la finalidad perseguida.

⁷⁹ STC 76/2019, Fundamento jurídico 7º a) p.27

⁸⁰ Artículo 5.1.a) RGPD y artículo 13 LOPDGD

Debido a esto se produce una violación de los principios de datos personales, concretamente el principio de minimización de los datos⁸¹.

Según la Circular 1/2019 AEPD, en ningún caso podrán ser objeto de tratamiento otro tipo de datos que no sean las opiniones políticas de las personas libremente expresadas por éstas en el ejercicio de sus derechos a la libertad ideológica y a la libertad de expresión, a los que, aplicando tecnologías como el tratamiento masivo o la inteligencia artificial, se pueda llegar a inferir su ideología política⁸². El TC en esta sentencia señala que tampoco se concreta si la recopilación se haría solo de páginas web y otras fuentes accesibles al público, o de otras fuentes.

A pesar de que la recopilación de datos ha quedado anulada por la STC 76/2019, la LOREG sigue permitiendo en el resto de apartados del art. 58. bis) tratamientos como la utilización para la realización de actividades políticas durante el período electoral, tal y como indica el apartado segundo. Sin embargo, la mencionada Circular señala que, de ninguna manera, dentro de ese tratamiento se incluye la comunicación o cesión de las opiniones políticas a terceros.

Respecto a quién puede recoger los datos relacionados con las opiniones políticas, el TC destaca que la disposición analizada no concreta si la recogida de las opiniones políticas la llevarán a cabo exclusivamente los partidos políticos o también podrán hacerlo federaciones, coaliciones y agrupaciones de electores, o incluso, si se podría encargar a un tercero⁸³. A esto da respuesta la Circular 1/2019 AEPD en su artículo dos apartados uno y dos, estableciendo que “estarán legitimados para el tratamiento de los datos, en el ámbito de la circunscripción que se corresponda con el proceso electoral al que se presenten, los partidos políticos, federaciones, coaliciones y agrupaciones de electores que presenten las correspondientes candidaturas y resulten proclamadas conforme a los artículos 43 y siguientes de la LOREG”⁸⁴.

En cuanto a cuándo se puede producir la recogida de las opiniones políticas o cuándo se podrán utilizar estas opiniones políticas⁸⁵, el precepto enjuiciado hace una breve

⁸¹ Principio reconocido en el art. 5.1. c) RGPD

⁸² AEPD, DEL, “Circular 1/2019, de 7 de marzo, sobre el tratamiento de datos..., op., Cit., p. 23

⁸³ STC 76/2019, Antecedente f) p. 7

⁸⁴ Arts. 2.1 y 2 Circular 1/2019 AEPD

⁸⁵ STC 76/2019, Antecedente f) p.7

referencia a las “actividades electorales”, vinculándolo a la “realización de actividades políticas durante el periodo electoral”. El TC resuelve considerando que el marco de las actividades políticas es demasiado amplio y genérico, ya que, además de que “los procesos electorales son relativamente frecuentes en nuestro sistema político”⁸⁶, dichas actividades pueden realizarse tanto durante la campaña electoral como en cualquier otro momento. A no ser que sea por razones de amenaza democrática, nada justifica una monitorización permanente de los datos personales de los electores⁸⁷.

Por último, el TC señala que en el artículo en cuestión tampoco se concretan las facultades de disposición y control de los datos cuya recopilación se autoriza, ni la entidad o sujeto que deberá darles respuesta. Esta cuestión la aborda la Circular de la AEPD en su artículo 11 apartado tercero, estableciendo que “deberá facilitarse de un modo sencillo y gratuito el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, con especial atención en el caso de este último, conforme al apartado 5 del artículo 58 bis de la LOREG”⁸⁸.

Teniendo en cuenta todos los motivos expuestos, el TC concluye que se produce inseguridad jurídica a los ciudadanos, partidos políticos y resto de operadores políticos, que contradice la exigencia de respetar el contenido esencial del derecho.

3.3. Garantías adecuadas

El tercer aspecto sobre el que versa la impugnación central gira en torno a la cuestión de si la norma impugnada ha previsto garantías adecuadas frente a la recopilación de datos personales que autoriza.

Por un lado, el Defensor del Pueblo sostiene que la propia ley habilitante ha de prever tales garantías, mientras que, por otro, el Abogado del Estado defiende lo contrario, sosteniendo que tales garantías se deducen tanto de la literalidad del precepto como de las normas que regulan la protección de datos personales en España, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018⁸⁹. De la lectura del artículo 58 bis).1 LOREG se

⁸⁶ STC 76/2019, Fundamento Jurídico 7º b) p.28

⁸⁷ GARCÍA SANZ, R. M. DEL, “Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público”, *Revista de Estudios Políticos*, nº 183, 2019, p. 129-159

⁸⁸ Artículo 11.3 Circular 1/2019 AEPD

⁸⁹ STC 76/2019, Fundamento Jurídico 7º c) p.29

extrae que se limita a señalar que la recogida de las opiniones políticas se producirá “únicamente cuando se ofrezcan las garantías adecuadas”.

Por tanto, el TC confirma, en primer lugar, que “las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado”, mientras que el precepto impugnado no remite expresamente a ninguna norma, sino que hace una referencia implícita al RGPD y a la LOPDGDD, lo cual, en su juicio, no es suficiente respecto de las exigencias constitucionales del principio de reserva de ley.

En segundo lugar, la inexistencia de unas garantías adecuadas deja vacío el contenido del derecho esencial, más aún cuando se trata de datos especialmente protegidos, que pueden comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad. El TC finaliza diciendo que “las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención”⁹⁰. El TC añade también que el nivel y la naturaleza de las garantías no se pueden determinar “de una vez por todas” ya que, por un lado, deben revisarse y actualizarse siempre que sea necesario y, por otro, que éstas deben cumplir con el principio de proporcionalidad y deben buscar nuevas posibilidades de tratamiento menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales⁹¹.

Para conocer, por tanto, cuáles serán las garantías adecuadas habría que remitirse a la Circular 1/2019 de la Agencia Española de Protección de datos, concretamente a su artículo 7.

⁹⁰ STC 76/2019, Fundamento jurídico 6º c) p. 23

⁹¹ STC 76/2019, Fundamento jurídico 6º c) p. 23 y 24

CONCLUSIONES

Como se ha mencionado durante todo el trabajo, el avance de las nuevas tecnologías es imparable, sobre todo en los últimos tiempos. Poco a poco va irrumpiendo en todos los ámbitos, y como era de esperar, también ha llegado a la política, donde la adaptación a los nuevos cambios y el desarrollo legislativo siempre irá unos pasos por detrás al desarrollo tecnológico.

La protección de datos personales es un derecho fundamental de todos los ciudadanos ya que supone una intromisión en su intimidad, razón por la cual han de estar perfectamente protegidos. Esta necesidad de protección se incrementa cuando los datos, además, son de carácter especial, como lo son el origen étnico o racial, las convicciones religiosas o filosóficas, o las opiniones políticas.

Los ciudadanos tienen que poder saber en todo momento qué está pasando con sus datos, para qué están siendo utilizados y de qué manera se han obtenido, siendo el consentimiento explícito para su uso es una de las características básicas que se establece en todos los textos legislativos que regulan esta materia. En el momento en que alguien se aproveche de la disposición de éstos y trate de “hacer negocio” con ellos, la confianza en la transparencia se perderá, y más si las personas que están detrás de estos actos son aquellos que ostentan poderes tan altos como el Gobierno del país.

Es cierto que existen precedentes en los que los datos obtenidos de los perfiles en las redes sociales de los ciudadanos han sido de gran utilidad a la hora de influenciar los resultados en las votaciones, ya que éstos te permiten crear propaganda individualizada en función de las opiniones y las interacciones de cada persona en su perfil, como ha sido el caso de Cambridge Analytica. Es por esto que considero que la introducción del artículo 58 bis) 1. LOREG, surgió de la idea de evitar que estas actuaciones se repitiesen, ya que debido a la velocidad con la que avanzan las nuevas tecnologías, se pueden generar lagunas normativas en situaciones que resultan completamente nuevas a los ojos de la ley.

La propuesta, como intención de incrementar los derechos de los ciudadanos y su protección frente a los distintos abusos, me parece que es necesaria y que, además, ha podido estar inspirada en corrientes europeas como la aprobación del Reglamento

2019/493, donde se incluía un procedimiento de verificación para comprobar si algún partido político europeo había influido o tratado de influir en el resultado de las elecciones al Parlamento Europeo, aprovechándose de una infracción de las normas, y de ser así, imponerle una sanción proporcionada y disuasoria.

El problema no surge de la idea como tal, sino de su planteamiento. Estoy de acuerdo en que un tema de tal trascendencia como son los derechos fundamentales ha de ser tratado y analizado profundamente, características que no se han tenido en cuenta en la propuesta presentada y que, con tal de ser aprobada con la mayor celeridad posible, ha dado lugar a un efecto contrario al pensado inicialmente, tanto a nivel legal, como a nivel de opinión pública.

El apartado impugnado, declarado inconstitucional por unanimidad, atentaba contra los intereses y derechos fundamentales, además de no establecer el interés público, las garantías, ni los límites del posible tratamiento, teniendo así la AEPD que emitir una Circular, complementada por el informe jurídico 210070/2018, concretando cuáles eran las garantías adecuadas a las que se hacía referencia, no siendo éste su papel sino el del legislador. Sin embargo, a pesar de estar tan claros los motivos de inconstitucionalidad tanto para el Defensor del Pueblo como para las Asociaciones que le solicitaron la interposición del recurso, no lo estaba tanto para el resto de los partidos políticos que componen las Cortes Generales, ya que la aprobación de la enmienda 331 propuesta por el Grupo Parlamentario Socialista obtuvo un amplio respaldo parlamentario.

El uso de las NTIC ha de suponer una ventaja a la hora de acercar la política a los ciudadanos y ayudar a favorecer su participación de una manera más libre y eficaz en la toma de decisiones políticas y elección de sus representantes. Para poder hacer efectiva esta participación, han de incrementar sus niveles de confianza en aquellos que les van a gobernar y, contrariamente a esta expectativa, como ya hemos mencionado, un 24,2% de los ciudadanos entrevistados declaró “no confiar nada” en los partidos políticos, hecho que se incrementa si, además, sabemos que éstos tienen la posibilidad de tratar nuestros datos personales más íntimos, sintiéndonos así más vulnerables y desprotegidos.

Pese a estos datos, en el Índice Mundial de Libertad Electoral realizado por la Fundación para el Avance de la Libertad, en el que se comparan 198 países, España ocupó el puesto

número 56 en 2018, con un total de casi 70 puntos sobre 100 en cuanto al desarrollo político, libertad de sufragio Activo y Pasivo y empoderamiento del elector⁹².

Verter opiniones en las redes sociales no ha de suponer un consentimiento implícito a que cualquier persona pueda hacer un uso inadecuado de éstas, y mucho menos aquellos que ostentan la Presidencia. Es por esto que han de existir normas claras y concretas, al igual que sanciones y controles expresos que logren un equilibrio entre los intereses de los partidos políticos y el respeto a la privacidad. Tal y como dice el Dictamen 3/2018 SEPD, se trata de plantearnos si queremos tener ciudadanos libres e informados, que opinen y participen, o sujetos cuantificables por lo que valen sus datos⁹³.

⁹² PEÑA, J. A. DEL, “Índice Mundial de Libertad Electoral”, *Fundación para el Avance de la Libertad*, 2018. Recuperado de: <http://www.fundalib.org/wp-content/uploads/2018/01/IMLE2018.pdf>

⁹³ Dictamen 3/2018 SEPD

BIBLIOGRAFÍA

Libros, artículos y revistas

- ABAJO, J. DEL, “2018 despide el año con un nuevo reglamento en materia de protección de datos”, *Derecho digital e Innovación Tecnológica H&A*, 2018.
- ADSUARA VARELA, B. /MARTÍNEZ MARTÍNEZ, R. DEL, “Debate sobre el nuevo artículo 58 bis de la LOREG”, *La Ley Privacidad*, nº1, *Diario la Ley (online)*, 2019.
- Centro de Investigaciones Sociológicas, DEL “Postelectoral elecciones Generales 2016”, *Distribuciones marginales*, 2016, p. 3.
Recuperado de:
http://www.cis.es/cis/export/sites/default/Archivos/Marginales/3140_3159/3145/es3145mar.pdf
- COLOMBO, C. DEL “Innovación democrática y TIC, ¿hacia una democracia participativa?”, *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 2006, p.29.
- GARCÍA JIMÉNEZ, L. DEL, “Reseña de “Democracia digital. Límites y oportunidades” de Cario Carou, H.”.
- GARCÍA MAHAMUT, R. DEL “Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español”, *Teoría y Realidad Constitucional*, nº35, 2015, p. 309-338.
- GARCÍA SANZ, R. M. DEL, “Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público”, *Revista de Estudios Políticos*, nº 183, 2019, p. 129-159
- GARRIDO CABEZAS, N. DEL. La construcción de una democracia digital, *Revista Latina*, 2010, p.5.
Recuperado de:
http://www.revistalatinacs.org/10SLCS/actas_2010/032_Norman.pdf
- GEORGES, M & KORFF, D. DEL “El Manual del Delegado de Protección de Datos. Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del RGPD”, *Agencia Española de Protección de Datos*, 2019.

- GÓMEZ DE AGREDA, A. DEL, “Falsas noticias, no noticias falsas”, *Telos: Cuadernos de comunicación e innovación*, 2018, p.1.
- GÓMEZ, R. M. DEL, “Principales novedades de la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (16), 2018, p. 201-246.
- HELD, D. DEL, *Modelos de democracia*. Madrid, Alianza Editorial, 2007, p. 336.
- HINOJOSA NAVARRO, G. DEL “Un intento de ciberdemocracia en España: el portal participativo “Decide Madrid” del Ayuntamiento de Madrid”. *Estudios sobre el Mensaje Periodístico*, 2019, vol. 25, no 2, p. 883.
- KAUFMAN, E. DEL, *E-Ciudadanía, prácticas de Buen Gobierno y TIC*, 2005.
- LÉVY, P. DEL, *Ciberdemocracia. Ensayo sobre filosofía política*, Barcelona, UOC, 2004, p. 10.
- LÓPEZ MARTÍNEZ, J. DEL, “Partidos políticos y datos personales de los ciudadanos. ¿Qué pueden usar y para qué?”, *SEPIN*, 2019.
- MAHAMUT, R. G., & CORDERO, J. V. DEL, “La protección de los datos personales de los solicitantes de protección internacional en el (nuevo) Sistema Europeo Común de Asilo: grandes desafíos y graves deficiencias”. *Teoría y realidad constitucional*, (44), 2019, p. 237-270.
- MARTÍNEZ-MARTÍNEZ, D. F. DEL, “Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones”, *El profesional de la información*, 27(1), 2018, p.185-194.
- MARTÍNEZ RODRÍGUEZ, J. DEL, “Participación política, democracia digital y e-ciudadanía para el protagonismo de adolescentes y jóvenes”, *Revista electrónica interuniversitaria de formación del profesorado*, 2011, vol. 37, no 14-2, p. 19-33.
- PEÑA, J. A. DEL, “Índice Mundial de Libertad Electoral”, *Fundación para el Avance de la Libertad*, 2018.
Recuperado de:
<http://www.fundalib.org/wp-content/uploads/2018/01/IMLE2018.pdf>
- PRODAT. DEL, “Boletín nº2 Febrero 2009”, *Boletín PRODAT*, 2009.
Recuperado de: <https://www.prodat.es/boletin/febrero2009/legislacion.html>

- RAMIRO ARENAS, M. DEL, “Partidos políticos, opiniones políticas e Internet: la lesión del derecho a la protección de datos personales”. *Teoría y realidad constitucional*, (44), 2019, 341-372.
- REIGADA, A. T. DEL, “Las redes sociales a la luz de la propuesta de Reglamento general de protección de datos personales: Parte uno”, *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, (15), 2012, p. 61-75.
- SUBIRATS, J. DEL, *Los dilemas de una relación inevitable: innovación democrática y tecnologías de la información y de la comunicación*” en CAIRO, H: *Democracia digital. Límites y oportunidades*, Madrid, Trotta, 2002, p. 91.

Legislación, jurisprudencia y otros instrumentos

- AEPD, DEL, “Circular 1/2019, de 7 de marzo, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la LOREG”, *Boletín Oficial del Estado*, 2019.
- Agencia Española de Protección de Datos (2019). Protección de Datos: Guía para el Ciudadano. Recuperado de <https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf>
- Arts. 2.1 y 2 Circular 1/2019 AEPD
- Artículo 5.1.a) RGPD y artículo 13 LOPDGDD
- Artículo 11.3 Circular 1/2019 AEPD
- Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311, art. 18.
- De España, G. Ministerio de Justicia, DEL, “Entrada en vigor del Protocolo nº16 al Convenio Europeo de Derechos Humanos”, *Área Internacional Portal Ministerio de Justicia*, 2019.

Recuperado de:

https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428869010?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DEntrada_en_vigor_del_Protocolo_n_16_al_Convenio_.PDF&blobheadervalue2=Docs_TEDH_Tribunal

- De Europa, C. DEL, “Convenio Europeo de Derechos Humanos, Tribunal Europeo de Derechos Humanos”, *F-67075 Strasbourg cedex*.
- De Europa, C. DEL, “Recomendación CM/Rec (2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles”, *Portal del Consejo de Europa*, 2010.
- De los Diputados, C. DEL, “Enmiendas e Índice de enmiendas al Articulado. 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, núm. 13.2”, *Boletín Oficial de las Cortes Generales*, 2018, p. 209. Recuperado de:
http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-2.PDF
- Del Estado, J. DEL, “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981”, *Boletín Oficial del Estado*, 1984.
- Del Estado, J. DEL, “Instrumento de Ratificación del Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001”, *Boletín Oficial del Estado*, 2001.
- Del Estado, J. DEL, “Ley Orgánica 5/1985, de 10 de junio, del Régimen Electoral General”, *Boletín Oficial del Estado*, 1985.
- Del Estado, J. DEL, “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”. *Boletín Oficial del Estado*, 294, 2018.
- DOUE. DEL, “Carta de los Derechos Fundamentales de la Unión Europea”, 2010.
- Europea, C. DEL, “Código de buenas prácticas en materia de desinformación”, *Policies, information and services*, 2018. Recuperado de:
<https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
- Europea, C. DEL, “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM (2018) 637 final”, *Diario Oficial de la Unión Europea*, 2018.

- Europea, C. DEL, “El código de buenas prácticas contra la desinformación cumple un año: las plataformas en línea presentan informes de autoevaluación, STATEMENT/19/6166”, *Declaración, Zona de Prensa*, 2019.
Recuperado de:
https://ec.europa.eu/commission/presscorner/detail/es/STATEMENT_19_6166
- Europea, C. DEL, “Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral, COM (2018) 638 final”, *Diario Oficial de la Unión Europea*, 2018.
- Europea, C. DEL, “Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal” COM 451 final, *Diario Oficial de la Unión Europea*, 2018.
- Europea, C. DEL, “Recomendación (UE) 2018/234 con vistas a reforzar el carácter europeo y el desarrollo eficiente de las elecciones de 2019 al Parlamento Europeo L45/40”, *Diario Oficial de la Unión Europea*, 2018.
- Europea, C. Para la democracia a través del Derecho. DEL “Informe conjunto de la Comisión de Venecia y de la Dirección de la Sociedad de la Información y lucha contra la delincuencia de la Dirección General de Derechos Humanos y Estado de Derecho sobre Tecnologías Digitales y Elecciones”, *CDL-AD (2019)016, Opinion No. 925/2018*, 2019. Recuperado de:
[http://www.cepc.gob.es/docs/default-source/comisionveneciadoc/cdl-ad\(2019\)016-e.pdf?sfvrsn=0](http://www.cepc.gob.es/docs/default-source/comisionveneciadoc/cdl-ad(2019)016-e.pdf?sfvrsn=0)
- Europea, U. DEL, “Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales ya la protección de la intimidad en el sector de las comunicaciones electrónicas”, *Diario Oficial de las Comunidades Europeas L*, 201, 2002.
- Europea, U. DEL, “Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)”. *Diario oficial de la Unión Europea*, 4. 2016.

- Europeo, P. y Consejo, DEL, “Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE”, *Diario Oficial de la Unión Europea*, 2018.
- Europeo, P. y Consejo, DEL, “Reglamento (UE, Euratom) 2019/493 por el que se modifica el Reglamento (UE, Euratom) n.º 1141/2014 en lo que respecta a un procedimiento de verificación relativo a las infracciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo L85 I/7”, *Diario Oficial de la Unión Europea*, 2019.
- Grupo de Trabajo sobre Protección de Datos del artículo 29. “Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679”. WP25rev.01, 17/ES, 2018.
- JEC, DEL, “Instrucción 3/2011 sobre interpretación de la prohibición de realización de campaña electoral incluida en el artículo 53 de la Ley Orgánica del Régimen Electoral General”, *Boletín Oficial del Estado*, 2011.
- JEC, DEL, “Instrucción 4/2007 sobre la utilización de las nuevas tecnologías de la información y de la comunicación electrónicas como instrumento de propaganda electoral”, *Boletín Oficial del Estado*, 2007.
- Ministerio de Justicia, DEL, “Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal”, *Boletín Oficial del Estado*, 2008.
- Of Europe, C. DEL, “Convention for the protection of individuals with regard to automatic processing of personal data”, *Directorate General of human Rights and Rule of Law*, 2017.
- Of Europe, C. DEL, “Resolution N.º 3 on data protection and privacy in the third millennium, MJU-30 RESOL,3E”, *30th Council of Europe Conference of Ministers of Justice*, 2010.
- Of Europe, C. DEL, “The modernised Convention 108: novelties in a nutshell”, *Diario Oficial de la Unión Europea*, 2018.
- SEPD. DEL, “Resumen del Dictamen del SEPD sobre el paquete de la Comisión relativo a unas elecciones europeas libres y justas”, *Diario Oficial de la Unión Europea C 47/8*, 2018.

- Supervisor Europeo de Protección de Datos. DEL, “El paquete de la Comisión relativo a unas elecciones europeas libres y justas, Dictamen 10/2018”, *Europe Publication*, 2018.
Recuperado de: https://edps.europa.eu/sites/edp/files/publication/18-12-18_opinion_on_election_package_en.pdf
- Supervisor Europeo de Protección de Datos. DEL, “La manipulación en línea y los datos personales, Dictamen 3/2018”, *Europe Publication*, 2018.
Recuperado de: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
- Supervisor Europeo de Protección de Datos. DEL, “Resumen del Dictamen del SEPD sobre la manipulación en línea y los datos personales”, *Diario Oficial de la Unión Europea C 233/8*, 2018.
- STC 76/2019, Antecedente f) p. 7
- STC 76/2019, Antecedente f) p.7
- STC 76/2019, Fundamento jurídico 6º c) p. 23
- STC 76/2019, Fundamento jurídico 7º a) p.27
- STC 76/2019, Fundamento Jurídico 7º b) p.28
- STC 76/2019, Fundamento Jurídico 7º c) p.29