derecom

ISSN: 1988-2629. Nº. 26. Nueva Época. Marzo 2019-Septiembre 2019

Cómo citar este texto:
Rosa María García Sanz. (2019). Cuestionando la protección del Reglamento Europeo de Datos Personales: algunos problemas identificados. *Derecom*, 26, 49-74. http://www.derecom.com/derecom/

CUESTIONANDO LA PROTECCION DEL REGLAMENTO EUROPEO DE DATOS PERSONALES: ALGUNOS PROBLEMAS IDENTIFICADOS

QUESTIONING THE PROTECTION OF EUROPEAN GENERAL DATA REGULATION: IDENTIFYING KEY PROBLEMS

© Rosa María García Sanz
Universidad Complutense de Madrid (España)
rosamaga@pdi.ucm.es

Resumen

El Reglamento Europeo de Protección de Datos contiene algunas disposiciones con una terminología muy ambigua, que permite una amplia interpretación y genera inseguridad jurídica. La vigente legislación electoral, concebida para un mundo analógico, no resuelve el desafiante escenario que la nueva tecnología plantea a la democracia. En este contexto, los partidos políticos disponen de normas en el Reglamento que permiten utilizar el genérico concepto de "interés público" como base jurídica para el tratamiento de datos personales en sus actividades electorales. Sólo estableciendo sólidas garantías jurídicas y técnicas, y una total transparencia, podrían evitarse usos excesivos, que podrían amenazar la integridad de los procesos democráticos y la misma democracia representativa.

Summary

General Data Protection Regulation provides several provisions that allow political parties to perform lawful processing of sensitive data based on very ambiguous terminology, such as "public interest". These provisions allow a wide range of interpretation, creating a lot of risks, such as inconsistency between published law and practice. In addition, a very powerful technology, which current electoral law does not contemplate, makes all these issues a very important challenge to democracy. Robust legal and technical measures along with absolute transparency over data processing must be provided. It could help prevent abuses and safeguard against some threats to representative democracy.

Recibido: 09/02/2019 Revisado: 04/03/2019
Aceptado: 05/03/2019 Publicado: 15/03/2019

Palabras clave: Protección de datos personales. Actividades electorales. Tratamiento de opiniones políticas. Vida privada.

Key words: Personal Data Protection Right; Electoral acitivities; Political opinions processing. Privacy.

1.Introducción.

EL Reglamento de Protección de Datos Personales[1] , cuya aplicación efectiva comenzó el 25 de Mayo 2018, contiene una previsión especial para los partidos políticos, en el ejercicio de actividades electorales, en cuanto al tratamiento de opiniones políticas, las cuales son datos personales categorizados como *sensibles* por esta ley. Con una enunciación en términos amplios, el considerando 56 y los correspondientes artículos del Reglamento provocan interrogantes y llaman a la reflexión en el contexto del Derecho de Protección de Datos y del Derecho Constitucional.

> *(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.*

Esta disposición establecida en términos abiertos y laxos permite un ámbito de tratamiento de los datos personales, por parte de los partidos políticos, que podría dañar los derechos fundamentales[2] de los ciudadanos en aras, supuestamente, de la democracia representativa y participativa, si no se dan auténticas garantías y controles, tanto en el Derecho de la Unión como en el de los Estados miembros[3] (Fernández- Miranda y Fernández Miranda, 2003:25).[4] Hay que partir de la premisa de que, conforme al estado del arte, la anonimización de los datos es prácticamente imposible (Ohm, 2010:1701-1716; Schwartz y Solove, 2011: 1877-78; Rosen, 2013)[5] y la re-identificación es posible siempre (Nissebaum y Barocas, 20014:49-50). Las *razones de interés público*, como base jurídica para el tratamiento de datos personales (art.6 del Reglamento), se presentan a lo largo del articulado justificando excepciones, exenciones y limitaciones al derecho fundamental de protección de datos personales.[6] Esta continua llamada al *interés público* podría dar cobertura legal a una gran variedad de prácticas de tratamiento de datos que, finalmente, podrían ser tan criticables como lo son las que se realizan en países[7] sin el reconocimiento de este derecho fundamental, y sin una legislación general estricta y garantista del derecho, en aras de la seguridad jurídica.

En la era de medios digitales en Internet, el *big data* y sus herramientas de análisis permiten obtener unas *conclusiones* que, utilizadas por partidos políticos sin escrúpulos, podrían llevar a la caricatura la teoría de la representación política. Sin embargo, el Reglamento podría contener, también, la llave para que los partidos políticos revitalicen sus funciones al servicio de la democracia. Podrían para ello renovar y transformar su relación con los medios de comunicación digitales *convencionales*, que también sufren una crisis de identidad y buscan la supervivencia. No siendo esto óbice, sino complementario, para el uso de las nuevas tecnologías, con todas sus bondades, para la comunicación directa de los partidos con los ciudadanos, y el fortalecimiento de los principios del trabajo parlamentario (Aranda, 2017:43). Lo cual, en definitiva, podría legitimar más que nunca la representación política.

El principio de legitimidad democrática, el pluralismo político y los partidos políticos (concebidos en el artículo 6 C.E. como *expresión del pluralismo político y como entes que concurren a la formación y manifestación de la voluntad popular y que son instrumento fundamental para la participación política*), pueden quedar falseados de contenido y pervertida su función si la vigilancia, recopilación y uso de los datos en relación con las opiniones políticas de los ciudadanos son el medio para manipular la formación de la voluntad popular, y dirigir la voluntad de voto socavando su libertad. La amenaza cobra más visos de realidad si recordamos que los otros grandes actores de la formación de la opinión pública, los medios de comunicación social, concebidos en su tradicional papel, sufren una crisis total por el impacto de las nuevas dinámicas comunicativas, consecuencia de Internet y sus recursos (García, 2017), como las redes sociales (las llamadas *fake news* son solo una de tantas anomalías). Los medios de comunicación social, los periódicos (digitales) por antonomasia, han dejado de ser el único intermediario o el exclusivo canal de comunicación entre los electores y los partidos políticos. Su relación ha cambiado: los partidos pueden comunicarse directamente con el elector (redes sociales, YouTube, emails, etc.) y el Parlamento puede expresarse por sí mismo también, estableciendo canales de comunicación directa con los representados,[8] (plataformas digitales, la IP Televisión, etc.). Sin embargo, podrían volver a necesitarse. No olvidemos que no solo las *máquinas* están pervirtiendo la llamada opinión pública en la Red, sino que a la vez existen detrás de ellas *profesionales activistas* (y otros agentes sin transparencia) que mueven todo ello para crear estados de opinión. La tensión entre democracia y representación política se exacerba.

Este trabajo se articula siguiendo los conceptos principales del citado considerando 56

2. Funcionamiento del sistema democrático y partidos políticos.

La democracia moderna es básicamente *democracia representativa*. La crisis de la representación democrática y la desconfianza entre representantes y representados se ha querido ver paliada y hasta resuelta por algunos estudiosos con el uso de las TIC (Tecnologías de la Información y Comunicación), uso que se hace tanto por los parlamentarios como por el Parlamento (Rubio, 2014; Aranda, 2017). La relación representativa ha permitido la discusión de los **asuntos públicos** en el Parlamento para la obtención del **interés general** mediante la negociación y el acuerdo político. Y es el funcionamiento democrático y el interés general (interés público) la razón esencial de las limitaciones establecidas en el Reglamento para el tratamiento de los datos especiales de opinión política. El artículo 23 sienta el principio general para los límites de este derecho fundamental:

> *23.1.El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una* ***medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) …c) e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés…***

La disposición, para no desnaturalizar el derecho fundamental, establece el respeto al *contenido esencial* y nombra los principios que el Tribunal de Derechos Humanos de Estrasburgo y el Tribunal de Justicia de la Unión Europea previamente han señalado, para que la norma que regule la vigilancia y el acceso a datos, a extramuros de la Ley general de protección de datos personales, sea conforme a los derechos fundamentales (criterios de necesidad, legitimidad, proporcionalidad, legalidad).[9] Ahora bien, queda, básicamente, en manos de los Estados aquilatar lo que debe ser *interés público* para el tratamiento de estos datos especiales y en lo que se entienda que requiere el *funcionamiento democrático*, así se lee en el artículo 6.2 del Reglamento:

> *6.2. Los Estados miembros podrán mantener o introducir **disposiciones más específicas** a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX…. 6.3.b.La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el **cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento**. Dicha base jurídica podrá contener **disposiciones específicas** para adaptar la aplicación de normas del presente Reglamento, entre otras…….:…. **El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido***.

Un estudio reciente de derecho comparado (Rubinstein et al., 2014:97)[10] ha analizado cómo usan los Estados (entre ellos algunos de la UE, como Alemania) estos mandatos genéricos de la Norma para una utilización de los datos poco transparente. Igualmente, ha detectado una desconexión posterior entre la ley y la práctica llevada a cabo por los poderes públicos que, por poco transparente, escapa a los controles (Ibíd.: 103). En principio debería pensarse, y debería ser así, que con esta ley y las bondades tecnológicas a su alcance, los partidos políticos están en la mejor situación de cumplir con su función constitucional (art.6 CE). Los mismos partidos, que siempre van a necesitar una base legal para tratar estos datos (art.6.2 del Reglamento), pueden encontrar, en los apartados 6.1.c), 6.1.e) y 6.1.f) del Reglamento, fundamentos para el tratamiento de los datos respecto a las opiniones de las personas, y, si es el partido en el Gobierno, podría recurrir a más razones convincentes e incluso a otros fundamentos. El rango de la posible ley, que disponga la base jurídica del tratamiento, podría ser una de las garantías para el respeto del derecho(s). Los mencionados apartados del artículo 6 señalan estos fundamentos que pueden utilizar los partidos:

> *6.1.c) el tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento; ..6.1.e) el tratamiento es necesario para el cumplimiento de una misión realizada en **interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; ..6.1.f) el tratamiento es necesario para la satisfacción de*

> ***intereses legítimos perseguidos por el responsable*** *del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado….*

No obstante, y a falta de norma específica, el artículo 6.4. pone a disposición otro recurso que sirva de base legal en el tratamiento de opiniones, escapando al control anterior:

> *6.4.Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una* ***sociedad democrática*** *para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable …..*

Pero aún más, el artículo 5.1.b) ofrece a los partidos políticos otra buena *baza* para tratar estos datos con base jurídica, y en conexión con el art. 9.2.d) e) y f):

> *5.1.b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)*;

Este precepto puede ser muy útil para el fin de generar bases de datos ideológicas y la posible creación de sicoperfiles, amén de otras utilidades que puede propiciar el *big data analytics*. En periodo electoral o en campaña permanente.

Teniendo en cuenta que los partidos políticos *concurren* a la formación de la opinión pública con los medios de comunicación social en un sistema democrático, esta disposición les podría inspirar para renovar su alianza con los medios convencionales, como los periódicos (digitales). Dado que la tradicional simbiosis entre medios de comunicación y partidos políticos[11] entró en crisis con la misma crisis de los medios de comunicación convencionales en el contexto Internet, ahora ambos se pueden volver a necesitar. Comparten un interés público imprescindible para el funcionamiento democrático, y no sería desatinado pensar en una colaboración basada en la citado considerando 56 del Reglamento. Ahora bien, cabría preguntarse, a qué partidos políticos se está refiriendo el Reglamento: a todos los registrados legalmente sin excepción; a todos los que se presentan a las elecciones o a los más significativos conforme a La ley electoral;[12] solo a los nacionales o también a los autonómicos y locales, siguiendo la misma Ley electoral; o únicamente a los que tienen representación parlamentaria. Si son estos últimos, particularmente, su actividad podría aliarse con la de los medios de comunicación con el fin de que la comunicación parlamentaria, que tiene una función política de *institucionalización de lo que ya es público, se realice adecuadamente y que se transmita con acierto y, a la vez, que sirva para que el Parlamento cobre un mayor protagonismo en la producción de la política* (Rubio y Vela, 2017a:112). Para hacer esto, en el contexto comunicativo de Internet, se requiere una sofisticada labor de observación y análisis para entender en cada momento cómo se produce la comunicación y se manifiestan las

opiniones e ideas en la red; para detectar allí la posible fragmentación y/o dispersión de opiniones y voluntades, y, en su caso, si se *modelan* con acciones como las de las *fake news* o incluso como consecuencia de vigilancia o espionaje *oculto* (exterior e interior). En esa misión compleja, trabajar junto a la *prensa* (sin ignorar la convergencia de medios de comunicación) puede ser muy eficaz para después identificar *intereses generales* y *espacios públicos comunes* con el fin de que los ciudadanos y electores ejerzan libremente sus derechos. Asimismo, los partidos políticos con representación parlamentaria, en el ejercicio de sus funciones y en el ámbito de la transparencia que hacen posible las Tics, en lo que se va llamando *parlamento abierto*, abren canales de comunicación directa con los ciudadanos a través de distintas herramientas (Rubio y Vela, 2017b).[13] En esas plataformas o canales quedan reflejadas las opiniones y datos de los representados en muy diversas cuestiones. ¿Qué pasa con esos datos? ¿Cómo se tratan? Si se conservan, ¿por quién, para qué y cuánto tiempo? Los partidos y los parlamentarios deberían informar con *transparencia* sobre todos estos puntos. E incluso se podrían diseñar estas plataformas para que la comunicación pudiera ser anónima (Martin y Fargo, 2015),[14] en la medida de lo posible técnicamente, si el ciudadano así lo desea. Sería una ironía que la pretendida transparencia y el aclamado derecho de acceso se convirtieran en una *trampa a la democracia*, debido a un uso de los datos que traspase los límites legales, solo en aras del *interés público* al servicio de la democracia. Al hilo de lo anterior surgen más preguntas: El partido en el Gobierno ¿juega con ventajas? ¿Afecta a la financiación de los partidos, por la compra y contratación de sofisticadas tecnologías y expertos en su empleo para estos fines?[15]

La concreción con que se determinen todos los extremos del tratamiento de opiniones tiene consecuencias distintas. Los partidos políticos cumplen un gran papel en el proceso democrático y en la organización política, al menos en la democracia que conocemos hasta ahora. Los partidos políticos no son poderes u órganos del Estado, pero conforme a la jurisprudencia del TC (STC 3/1981) son asociaciones políticas que llevan a cabo funciones públicas. De acuerdo con ello, es posible atraer distintos artículos del Reglamento que se refieren a personas o instituciones en el ejercicio de poderes o funciones públicas para el tratamiento de datos (art.6.2). Consecuencia directa de la representación parlamentaria, es la democracia **un procedimiento y unas reglas** para la elección de representantes y gobernantes, **una manera de organización política e incluso un valor constitucional** (preámbulo de la CE, art. 1). Sin olvidar la prohibición constitucional del mandato imperativo (art.67.2 CE) que obliga a los elegidos a representar a **toda** la población **y no solo a sus electores concretos**. Dicho esto, el acceso y manejo de datos políticos de los electores es un asunto nuclear para dicho proceso democrático y para la representación parlamentaria. Y puede quedar muy comprometido si no se establece y articula afinadamente qué tratamiento es legal: qué partidos (y qué órganos o personas del partido son responsables del tratamiento) y en qué situaciones concretas pueden recopilar esos datos y qué operaciones a realizar en su tratamiento;[16] de qué origen y fuentes pueden recopilar y tratar (medios de comunicación social, redes sociales, perfiles y mensajes públicos o privados, motores de búsqueda y sus resultados, cookies propias y ajenas, acceder a los metadatos de los móviles en reuniones y manifestaciones políticas, bases de datos públicas y/o privadas, etc.), con qué herramientas, durante cuánto tiempo pueden recopilar, y cuánto tiempo deben almacenar esos datos (si es en la *nube*, con qué seguridad); si pueden recibir la colaboración de las compañías tecnológicas[17] o de los medios de comunicación, qué tipo de algoritmos e inteligencia artificial pueden utilizar y si se les permite realizar perfiles para tomar decisiones y *discriminar* conforme a las opiniones de diferentes sectores de la sociedad, etc.. El análisis que se realiza del *big data* ofrece correlaciones, no causas (Cukier y Mayer-Schoenberger, 2013: 29, 37),[18] y la toma de decisiones para el interés general requiere saber los *por qué* para ofrecer políticas y legislaciones correctas que incluyan a todos sin discriminar. La clásica función de los partidos de reducir la complejidad (Fernández Miranda y Fernández Miranda, 2003:32-33)[19] en un

sistema democrático, que podría haberse visto comprometida en principio (por la fragmentación, dispersión y burbujas de opinión en la Red y en la calle), podría reafirmarse de nuevo, finalmente, si los partidos se reinventan en este sentido. Ahora bien, deben estar advertidos de que el *big data analytics* y algunas herramientas diseñadas para el análisis político electoral, pueden identificar a cada votante y su perfil opinático (incluso perfiles psicológicos). Ello permite fraccionar la sociedad y comunicar mensajes a medida de cada votante individual con el fin electoral que se persiga. Y, finalmente, reconducir todo para uniformar el pensamiento o, si es el caso, certificar el pensamiento uniforme que se ha generado. Las nuevas tecnologías de la información -*software,* algoritmos (Reitinger, 2016)[20] y/o la inteligencia artificial para el tratamiento autónomo y automatizado de los datos y/o el *big data analytics*-, a disposición según el estado del arte, lo posibilitan si no se dan las garantías y los controles necesarios. El pluralismo político-ideológico que caracteriza la democracia contemporánea podría desvanecerse, así como el imperio de la ley en tanto que expresión de la voluntad general (pues la voluntad del pueblo puede no ser ya la del pueblo). Sin una revitalización de los partidos, conforme a los nuevos tiempos, con todos las garantías legales y controles técnicos, éstos podrían convertirse en otros manipuladores más de las opiniones; o, sencillamente en meras correas de transmisión para certificar las opiniones fruto de ciertas prácticas comunicativas (perversas) en Internet (*fake news,* burbujas de opinión de las redes, fragmentación, consecuencia de identificación de perfiles, psicoperfiles, vigilancia de comportamientos, etc.) (Rubio y Vela, 2017a: 109).[21]

Sin embargo, el Reglamento y la tecnología ofrecen, asimismo, la oportunidad a los partidos políticos de *actualizar* sus funciones y *reinventar* su relación con los medios de comunicación *convencionales* en Internet, sin ignorar, a la vez, la relación directa con los ciudadanos: podrían desenmascarar los *falsos* estados de opinión mediante el *big data* y su análisis por algoritmos y/o inteligencia artificial; podrían conectar con las opiniones de las mayorías y de las minorías y crear un debate público común para que después, con representación parlamentaria, se persiga mejor y más afinadamente los intereses generales de todos, sin ignorar a las minorías. Obviamente, de nuevo, se exige que la norma concreta que autorice esa recopilación y tratamiento de datos opináticos (que debería ser una ley orgánica por los distintos derechos fundamentales en juego) afine muy bien los términos legales y medios tecnológicos implicados para que estos puedan perseguir el fin democrático con éxito. No hay que olvidar que existe una tecnología capaz de ignorar la ley y vulnerar el derecho a la protección de datos. Tratar estos aspectos parciales, aunque radicalmente fundamentales, de la democracia centrada en Internet, está haciendo una llamada de principio, que en algún momento habrá que abordar, respecto a la construcción jurídica de la democracia digital.

Si la democracia representativa tiene como objeto garantizar que todos los ciudadanos participen en libertad e igualdad en las elecciones y en la vida pública, el uso pervertido de los datos y sin respeto de los derechos fundamentales (p.e. de la privacidad), puede corromper el sistema democrático desde su mismo núcleo. Y aunque los ciudadanos tienen reconocido su derecho de acceso a los documentos, archivos y registros públicos de los poderes públicos (Ley de Transparencia ya citada en nota 7) y a la transparencia respecto al tratamiento de sus datos personales (Reglamento, artículo 12) puede no ser suficiente para el efectivo control del poder político, pues los partidos, especialmente, el partido en el poder, pueden ejercer una publicidad proactiva (Ley de Transparencia), acorde con *las tendencias predominantes de opinión* observadas sin despertar sospecha y sabiendo manipular a las minorías.

De acuerdo con la Constitución, los partidos políticos son instrumento fundamental para la participación política (art.6 CE). Pero son eso, el instrumento, que no titulares del

derecho de participación del que son los ciudadanos mismos titulares, según doctrina del Tribunal Constitucional (STC 64/2002).En el preámbulo de la CE queda manifiestamente claro el valor superior que representa el pluralismo político (art. 1 y art.6) y la importancia de los partidos políticos para su formación y expresión como instrumentos clave de la participación política. La misma Constitución consagra la participación ciudadana, a la que los partidos políticos sirven de instrumento, a tres niveles: como principio estructural (art.9), como derecho fundamental (art. 23) y como un conjunto institucional (órganos constitucionales y asociaciones con funciones públicas) (Aparicio, 2009: 116). La recopilación y tratamiento de los datos personales, respetando la Constitución y los derechos fundamentales de los ciudadanos, por parte de los partidos, significa el respeto mismo a la democracia representativa. De no hacerlo así, significaría un suicidio institucional por parte de los propios partidos, pues como asociaciones requieren de los derechos de privacidad, de información y expresión libre, entre otros, para asegurar su pervivencia (Schwartz, 1995). Si se aniquila la privacidad de las personas (incluida la de los partidos y sus miembros) se aniquila la misma libertad como derecho, y el mismo presupuesto del ejercicio de los otros derechos (Rallo Lombarte, 2017).

3. Actividades electorales

La Ley Orgánica Electoral (ya citada en nota 11) define la **campaña electoral** en el artículo 50.4.

> *Se entiende por campaña electoral, a efectos de esta Ley, el conjunto de actividades lícitas llevadas a cabo por los /**candidatos, partidos, federaciones, coaliciones o agrupaciones** en orden a la captación de sufragios. 5. Salvo lo dispuesto en el apartado 1 de este artículo, ninguna persona jurídica distinta de las mencionadas en el apartado anterior podrá realizar campaña electoral a partir de la fecha de la convocatoria de las elecciones, **sin perjuicio de lo establecido en el artículo 20 de la Constitución**.*

En el artículo 51 limita de manera estricta la campaña temporalmente. Y respecto a la **propaganda electoral** se refiere en el artículo 53 de la misma:

> *Período de prohibición de campaña electoral. No puede difundirse propaganda electoral ni realizarse **acto alguno de campaña electoral** una vez que ésta haya legalmente terminado. La obtención gratuita de medios proporcionados por las Administraciones Públicas quedará limitada al periodo estricto de campaña electoral. Las limitaciones anteriores se establecen sin perjuicio de las actividades realizadas por los partidos, coaliciones y federaciones en el ejercicio de sus funciones constitucionalmente reconocidas y, en particular, **en el artículo 20 de la Constitución.** No obstante lo anterior, desde la **convocatoria de las elecciones hasta el inicio legal de la campaña**, queda **prohibida** la realización de publicidad o **propaganda electoral mediante carteles, soportes comerciales o inserciones en prensa, radio u otros medios digitales,** no pudiendo justificarse dichas actuaciones por el ejercicio de las actividades ordinarias de los partidos, coaliciones o federaciones reconocidas en el apartado anterior*.

La Ley no diferencia con claridad *la campaña electoral* de la *propaganda electoral*, pero sí delimita con precisión el tiempo de la campaña electoral dentro del periodo electoral. Y se refiere, en todo caso, a las ideas, opiniones políticas o actos en campaña electoral, que pueden emitir los candidatos y partidos políticos, pero nada dice de las expresadas por los electores. El considerando (56) del Reglamento de Datos se encabeza con ***si, en el marco de actividades electorales***, lo que parece reclamar una mayor concreción sobre si se trata únicamente de actividades estrictamente electorales durante la campaña electoral (nacional, autonómica o local), o sobre actividades que se califican como electorales y se dirigen al fin general electoral de una manera más amplia, pero pueden sobrepasar ese límite legal. En otras palabras, qué es a*ctividad electoral* y si la recopilación de datos de opinión de los electores podría ser un *acto de campaña electoral* estrictamente (art. 53 Ley Electoral) o podría calificarse como *actividad electoral* en sentido más general, en tiempo y contenido. Indudablemente de la lectura del Reglamento surgen preguntas y algunas no menores: sobre qué actividades electorales, si en campaña o en periodo electoral solo, o si incluso en tiempo no electoral pero con fines electorales; o si los datos se destruyen después de la campaña. Especial interés provoca el partido en el Gobierno, sobre si tiene acceso continuo a las opiniones políticas y mediante qué medios y para qué fin. A la campaña electoral, estrictamente, quedan limitados los recursos que de las Administraciones Públicas pueden obtener los partidos. Y en una interpretación sistemática de la Ley electoral con el Reglamento de datos, cabría plantearse si la Administración podría, en este sentido, proporcionar los recursos de recopilación y tratamiento de datos de los ciudadanos a los partidos, en régimen de igualdad durante ese periodo. La ley electoral poco más dice acerca de la *propaganda electoral* o *publicidad política* o *actividades electorales*, tomando los términos allí utilizados. Luego de ello puede vislumbrarse un amplio espectro de posibilidades. La materialización de lo que es propaganda electoral (o no) ya no se limita a los mensajes explícitos (del pasado), y hay muchas formas y formatos de llevarla a cabo de una manera continuada, latente y no explícita (Jason, 2015:46).[22] Al amparo del ejercicio del artículo 20 CE, es posible una ilimitada actividad comunicativa con finalidad electoral, tanto en las redes sociales como a través de otros recursos (*blogs*, plataformas, *chats,* etc.), sin vulnerar la vigente ley.[23] Por otra parte, los algoritmos y la inteligencia artificial pueden realizar una labor muy productiva a este respecto, sin necesidad de explicitar mensajes electorales, sino examinando los comportamientos de los ciudadanos en la Red (Kosinski et al., 2013),[24] difundiendo información *ad hoc* según sus perfiles y, quizá ya en campaña electoral, exponiendo a estos distintos segmentos de población identificados mensajes claramente propagandísticos. Todo ello conforme a la legalidad. Se diría que la propaganda se ha liberado del *corsé legal* de la campaña electoral y puede manifestarse de otras maneras, incluso más efectivas. Parafraseando a Stanley Jason, *la propaganda peligrosa en una sociedad democrática es aquella que no es reconocida como propaganda* (Jason, 2015:46).

La Junta Electoral Central ha publicado dos Instrucciones que podrían tener aquí alguna relevancia (INSTRUCCIÓN 4/2007, de 12 de abril, de la Junta Electoral Central, sobre la utilización de las nuevas tecnologías de la información y de la comunicación electrónica como instrumento de propaganda electoral. E INSTRUCCIÓN 3/2011, de 24 de marzo, de la Junta Electoral Central, sobre interpretación de la prohibición de realización de campaña electoral incluida en el artículo 53 de la LOREG). Sin embargo, ni en estas Instrucciones ni en la doctrina de la Junta Electoral Central[25] se aborda con profundidad y realismo el papel de los nuevos medios de Internet en la propaganda electoral, como tampoco la cuestión del uso de los datos políticos de los ciudadanos en función del proceso electoral o de la campaña electoral, salvo lo referido a los datos del censo electoral.

Una nueva ley electoral debería contemplar estos extremos, observando con realismo todo el escenario que ofrece Internet, tanto en *propaganda* como en la utilización de los datos personales de los ciudadanos. El tratamiento de datos personales tomados de todas las *fuentes posibles* en Internet, ha trasladado el verdadero *campo de batalla electoral* a la Red.[26] Y ello sobrepasa los límites, los medios y las maneras de la campaña electoral diseñada en la vigente Ley, que la proyecta en *analógico*. Es decir, pensada básicamente *en* y *con* los medios de comunicación social convencionales y con propaganda evidentemente convencional, a pesar de que haya un intento, poco fructífero por otra parte, de extender la Ley electoral vigente a los medios electrónicos. Se requiere una nueva ley, ya en sede de protección de datos personales ya en sede del sistema electoral, donde se aborden expresamente todas estas nuevas realidades, conscientes de que *lo obvio* no es el escenario de los nuevos tratamientos de datos por las nuevas tecnologías. En definitiva, una nueva ley debería establecer las garantías necesarias para preservar la integridad del proceso democrático, en consonancia con las nuevas *bondades* y *amenazas* de la Red.

4.Opiniones políticas

El Reglamento establece una prohibición general del tratamiento de opiniones políticas, la cual, después, en el mismo texto, es susceptible de importantes excepciones en aras del interés público. Esto, unido a la ambigüedad de lo que debe entenderse por *qué observar o cómo extraer las opiniones políticas* en el ecosistema Internet, con todas las herramientas técnicas disponibles, llama a una mayor determinación de lo que debe entenderse por *el tratamiento de opiniones políticas* por parte de los partidos políticos en una sociedad democrática. Veamos estas disposiciones y algunas de sus implicaciones:

El art. 9.1. del Reglamento establece:

> *1.Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial,* ***las opiniones políticas,*** *las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.*

Sin embargo, ya el considerando 52 adelantaba:

> *(52) :* ***Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales*** *cuando lo establezca el Derecho de la Unión o de los Estados miembros …*

Y el mismo **artículo 9.2. d) establece que la prohibición general no se aplica**, extendiendo más el círculo de excepciones:

> *9.2.d) cuando el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una* ***asociación*** *o cualquier otro organismo sin ánimo de lucro,* ***cuya finalidad sea política,*** *filosófica, religiosa o sindical, siempre que el tratamiento se refiera* ***exclusivamente a los miembros actuales o antiguos de tales***

organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

El tenor literal de la anterior excepción señala *personas que mantengan contactos regulares* y, tratándose de partidos políticos, se podría dar una interpretación muy amplia a esta expresión vaga y ambigua del precepto. Igualmente, convendría aquilatar qué se entiende por *opiniones políticas*: si se permite obtener solo los meros datos o también los contenidos donde están esos datos; de dónde y de qué contextos se pueden recopilar. Aunque se puede contestar técnicamente qué es un mensaje de opinión (García Sanz, 1990), la realidad digital muestra que hay muchas maneras, elementos, comportamientos, datos (en definitiva) en la red que, procesados mediante *software*, algoritmos o inteligencia artificial, son capaces de destilar todas las opiniones e ideas políticas (y no políticas) de un usuario. De dónde extraen las opiniones políticas los partidos políticos: Bases de datos públicas o también de organizaciones privadas; cómo y con qué instrumentos las tratan (*big data analytics,* algoritmos gobernantes o inteligencia artificial); con qué extensión y duración. Los partidos podrían ponderar varias opciones para recopilarlas: -Directamente del interesado –Indirectamente por otras fuentes, públicas o privadas .[27] Con consentimiento o sin consentimiento, por razones de interés público (o de investigación y estadística), en ambos supuestos. Y así seguir considerando más posibilidades, de las que se pueden mencionar algunos ejemplos:

• Observar y recopilar las opiniones políticas de los perfiles y mensajes públicos de las redes sociales y de todo tipo de medios de comunicación y bases de datos, dentro y fuera de la red (fuentes públicas).

• Poder tener acceso, por razones de interés público democrático, incluso por razones estadísticas y de investigación, no solo a los datos públicos personales sino incluso a los privados.

• Hacerlo como responsables del tratamiento pero con encargados del tratamiento que pueden ser académicos e investigadores e incluso medios de comunicación. O al revés, que sean los estudiosos o investigadores los responsables del tratamiento, pero después, y digamos por razones de interés púbico democrático, acceder a los datos y su tratamiento para fines electorales.

Y sin olvidar lo que advierte el considerando 61 sobre los deberes de información a los interesados, tanto si se obtienen los datos de ellos directamente o de otra fuente. Igualmente si se comunican legítimamente a otro destinatario o si se tratan para un fin diferente al inicial.

Parece -ya no es una sorpresa- que ley y tecnología, conforme el estado del arte, posibilitan estrategias y acciones previsibles e imprevisibles (Weber y Wong, 2017), (cuya base jurídica de tratamiento puede ser otra distinta del consentimiento e informar de las mismas al ciudadano a posteriori puede no ser muy eficaz). Y a efectos de actividades electorales y representativas, reconocer que bien se puede *observar y certificar* un estado de opinión (que bien puede haber sido manipulado y creado en Internet mediante técnicas que permiten el conocimiento emocional de cada votante y al que se le ha podido o se puede influir incluso individualmente) o bien se puede realizar por los partidos esa labor de influencia y creación de opinión. Obviamente, todo debería hacerse conforme a los derechos fundamentales, que se deben respetar en un Estado democrático y, por supuesto, entre otros, el derecho a la

privacidad (Rallo Lombarte, 2017: 595), cuya vulneración para fines electorales debería estar muy justificada por razones de *interés general*. El Reglamento no ignora la capacidad de la técnica de *vulnerar continuamente* la privacidad de las personas, como bien señala el considerando 30:

> *(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.*

Pero aún más, inaplicando la prohibición general, hay más disposiciones que son aplicables al caso, de las que se pueden valer los partidos políticos para el tratamiento legal de opiniones:

> *Art. 9.2.e) cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho …j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1. ..*

Todo ello podría dar cobertura legal a posibles actividades de tratamiento de las opiniones políticas por los partidos: utilizando las herramientas que recoge el considerando 62, y otras muchas disponibles, para recabar e identificar las opiniones y las personas, sin perjuicio de la posible anonimización o seudoanonimización. Incluso una ley podría autorizar al efecto, con las garantías que establece el Reglamento, acuerdos con las grandes empresas tecnológicas (incluso otras instituciones) para tener acceso o compartir datos pertinentes con la finalidad electoral de interés público.

Así pues, parece que más que el concepto, es la manifestación misma o expresión de la opinión política en Internet la que merece una reflexión que la acote o concrete. No se puede ignorar que es posible prever la opinión política, por ejemplo, del seguimiento de los distintos movimientos del usuario en la red (psicoperfiles). De modo que su espectro podría ser muy limitado o muy amplio si se recoge una heterogénea gama de seguimientos, expresiones, creencias, ideas de todo tipo, de materias y temas, etc.. Luego, podrían comprenderse como opinión política más tipos de datos, y más de los que se incluyen en la categoría de datos especiales. En definitiva, hay aspectos que merecen ser aclarados, en aras de la seguridad y garantías jurídicas.

En este sentido, debería reflexionarse si hay que considerar solo las opiniones (políticas) publicadas u opinión pública inducida de los medios de comunicación periodísticos u otros medios de comunicación o redes sociales y otros recursos electrónicos. Si deberíamos entender que las opiniones publicadas y sumadas de los ciudadanos individualmente (como en las redes sociales) constituyen la opinión pública o interés público general. Si solo las opiniones publicadas o manifestadas públicamente o también manifestadas en privado (Weber y Wong, 2017.),[28] extraídas tanto de los medios convencionales como de las redes sociales, YouTube,

chats, blogs, buscadores, etc.… Si se deben utilizar *cookies* para trazar líneas de comportamiento y perfiles de opinión. O los algoritmos e inteligencia artificial para crear categorías y perfiles sobre los que tomar decisiones o líneas de actuación. Si se consideran solo las opiniones políticas de sus afiliados, de su electorado o de toda la sociedad. La excepción de interés público podría cubrir una gran variedad de posibilidades. Y las medidas de seguridad deben extremarse cuantas más personas estén expuestas, pues la vulneración de los datos especiales o sensibles puede causar daños impredecibles.[29] En este sentido, hay que atender al Reglamento:

> *(71)….. **asegurar los datos personales** de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, **efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical,** condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. **Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones especificas.***

El pluralismo político como principio estructural tiene una gran relevancia institucional (Aparicio, p. 118). Pero ese pluralismo político puede verse pervertido y falseado con una manipulación de los datos.

5. Razones de interés público

El fin del i*nterés público*- junto a otros fines que explican Rubinstein y otros autores (2014:1 y ss.)-, como la seguridad nacional, seguridad pública, la lucha contra el terrorismo, la persecución del crimen, el cumplimiento de las normas, razones administrativas, el cumplimiento fiscal o razones democráticas, etc., se repiten tanto en las leyes de protección de datos como en aquellas extramuros de éstas, que autorizan al Estado y a los poderes públicos un mayor margen de maniobra en el tratamiento de datos, sin someterse a las garantías y controles de las mismas (Rubinstein et al, 2014:97).[30] De tal manera que concluyen los referidos autores:

> "*Here is this paper's basic conclusion: In most if not all countries, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level. At the practical level, the law provides little guidance, leaving companies to fill the gaps with their own judgments. From the human rights perspective, the systematic access that governments obtain is not foreseeable from the text of the law, calling into question whether the laws in many countries meet evolving human rights standards*" (Rubinstein et al, 2014: 97).

Efectivamente, en el Reglamento objeto de estudio, tanto en su artículo 2.1.d), por el ámbito de aplicación material, como en distintos artículos a lo largo del mismo, se introducen

esas finalidades que permiten la no aplicación o el establecimiento de límites y excepciones del Reglamento. Los riesgos que pudieran derivarse, no solo afectan al propio país sino incluso más allá de la propia U.E. (art.2.1.a) por la naturaleza global de Internet. A modo de muestra, aunque, obviamente, no exhaustiva, se citan y/o se ofrecen algunos extractos del Reglamento donde se hace la llamada continua al fin del *interés público.*[31] Puede dar una idea del amplio espectro de actividades y posibilidades que abre en el acceso y uso de los datos políticos y sociales. El término *interés público* expresado de forma vaga y ambigua requiere una específica concreción en cada caso, que evite decisiones discrecionales que deberían controlarse por parte de las Autoridades de Datos. E igualmente, en este sentido, cumplir escrupulosamente, en la medida posible, con las garantías que prevé el propio Reglamento con el fin de evitar posibles vulneraciones de los derechos fundamentales.

Al final del texto se han citado artículos y reproducido algunos considerandos del Reglamento sobre la base jurídica del tratamiento en *interés público* necesario para una *sociedad democrática*. Sin embargo, se reproduce, aquí en el texto, parcialmente, los artículos 23 y 6, que representan fielmente cómo diseña el legislador el uso de esta base jurídica de tratamiento.

> *Art.23.1 1.El Derecho de la Unión o de los Estados miembros que se aplique al o el encargado del tratamiento p**odrá limitar, a través de medidas legislativas**, el alcance de las obligaciones …., cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una **sociedad democrática** para salvaguardar: a)… f) **objetivo de interés público general…**.*

También el artículo 6 establece las circunstancias del tratamiento sobre la base jurídica de *interés público*, tanto en los apartados 6.1.c) y e), ya citados, como en los siguientes:

> *6.3 3.La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: ……. necesaria para el cumplimiento de una misión realizada en **interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. …… El Derecho de la Unión o de los Estados miembros cumplirá un **objetivo de interés público** y será proporcional al fin legítimo perseguido.*

Y esto en conexión con el art. 6.2 que autoriza a los Estados a establecer en su Derecho normas específicas respecto al *cumplimiento de una obligación legal, el **interés público o en el ejercicio de poderes públicos*.** También se trae a colación aquí el art.6.4, que atiende a las necesidades de una ***sociedad democrática*** como base jurídica principal del tratamiento, y que debería observar los objetivos del artículo 23, entre los que se encuentran ***el interés público*:**

6. Las garantías adecuadas

El artículo 23.1, ya reproducido, enumera los límites a los derechos establecidos en el Reglamento, aunque no parece ser una lista cerrada. Y, asimismo, a continuación, en el artículo 23.2 establece las garantías que deberán ofrecer las normas específicas que establezcan tales excepciones o límites:

> *23.2.En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones*

> *específicas relativas a: a) la finalidad del tratamiento* ***o de las categorías de tratamiento****; b)* ***las categorías de datos personales*** *de que se trate; c) el alcance de las limitaciones establecidas; d) las garantías para evitar accesos o transferencias ilícitos o abusivos; e) la determinación del responsable o de categorías de responsables; f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento; g) los riesgos para los derechos y libertades de los interesados, y h) el derecho de los interesados a ser informados sobre la limitación,* ***salvo si puede ser perjudicial a los fines de esta.*** (La negrita es de la autora, para llamar la atención de que al hablar de *categorías* hay una pérdida importante de control. Y, también, para llamar la atención sobre esa *salvedad* que, en el caso que nos ocupa, no debiera contemplarse nunca).

Se extrae de la disposición legal, interpretada sistemáticamente con el resto del Reglamento, que se requieren medidas legales, técnicas y organizativas que garanticen la legalidad de estos tratamientos excepcionales (Rubinstein et al, 2014:114).[32]

• Técnicas y organizativas: Medidas de seguridad proactivas.

Conforme al RGPD, artículos 32, 33 y 34, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en un análisis previo.[33] En general, siempre las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve, y, en consecuencia, podría ser suficiente con medidas de protección de datos desde el diseño o con otras medidas de seguridad suficiente. Pero igualmente, las medidas organizativas y técnicas a implementar dependerán del coste de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos para los derechos y libertades. Dado que los riesgos para los derechos y libertades parecen muy posibles y elevados (se tratan datos especiales), los costes, quizá excesivos para algunos partidos, no deberían ser una excusa para la no implantación de medidas (y tienen el deber de consultar a la autoridad competente). En consecuencia, los partidos políticos deberán realizar así, en primer lugar, un análisis de los riesgos en relación con los derechos y libertades, previo al inicio de los tratamientos. Para valorar estos riesgos deberán considerar los tipos de tratamiento, la naturaleza de los datos, el número de interesados afectados, la cantidad y variedad de tratamientos que una misma organización realice y las tecnologías que utilice, etc. Según el tamaño de la organización, de la naturaleza sensible de los datos o de la complejidad de los tratamientos, puede generarse una mayor o menor obligación de medidas de seguridad y organizativas por parte de los partidos políticos. Teniendo en cuenta que éstos suelen ser organizaciones numerosas, que tratan opiniones políticas (datos sensibles o especiales) y que afectan a un gran número de personas, podrían estar no solo obligados a realizar un análisis de riesgos sino también lo que se llama en el Reglamento *un análisis de impacto* (evaluaciones de impacto sobre la protección de datos, EIPD), conforme al artículo 35, dado el alto riesgo de lesión de derechos y libertades de las personas en los tratamientos. Podrían, por tanto, necesitar tecnología adecuada para la protección y seguridad de estos datos, tales como la minimización, anonimización o seudoanonimización de los datos, el cifrado o criptología, y la presencia humana cuando se trate de inteligencia artificial y/o algoritmos que puedan tomar

decisiones automatizadas o realizar perfiles sobre las personas (art. 22.3). Salvo que conforme al art.22.2.b), una disposición legal levante la prohibición general de *no ser objeto de una decisión basada en el tratamiento automatizado*. Se establece, en principio, respecto a las opiniones políticas, la prohibición general de tomar decisiones automatizadas y de elaboración de perfiles basados en datos especiales, salvo que se atienda a las excepciones del artículo 22.4. De manera que, aplicando las *salvedades* que excepcionan la prohibición general, es posible la toma de decisiones automatizadas y la elaboración de perfiles con datos especiales si es por razón de interés público, como es al caso de las opiniones políticas (art.22.3). Véase lo anterior, también, en relación con el artículo 89 del Reglamento (razones de investigación, estadística o archivo).

Puede resultar esclarecedor lo que detalla el considerando 71 del Reglamento en relación con la elaboración de perfiles y las decisiones automatizadas:

> *A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la* ***elaboración de perfiles,*** *aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes …….y se impidan, entre otras cosas,* ***efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical,*** *condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.* ***Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.***

Igualmente, los partidos deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que responda a cuestiones como: nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese, finalidades del tratamiento, descripción de categorías de interesados y categorías de datos personales tratados, transferencias internacionales de datos… De esta obligación de registro están exentas las organizaciones que empleen a menos de 250 personas, salvo que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, que no sea ocasional o incluya categorías especiales de datos, como los datos políticos en este caso. Igualmente, deben establecer, conforme al Reglamento, los procedimientos adecuados para notificar las quiebras de seguridad a los ciudadanos cuando se produzcan, con las salvedades que establece la ley. También los partidos políticos, al realizar actividades en interés público, tratando datos sensibles y normalmente a gran escala, que pueden exigir una continua vigilancia, deberían nombrar, conforme a la ley, la figura del Delegado de Protección de Datos.

Los partidos, por tanto, deberían valorar, previamente, sus posibilidades, antes de emprender tratamientos que les exijan unos recursos para proteger los datos y derechos de los ciudadanos, recursos de los que, posiblemente, no disponen. Esto, obviamente, puede colocar a unos partidos en ventaja respecto a otros, y *jugar en el terreno político* sin igualdad de condiciones.

• Legales: medidas legislativas específicas para el tratamiento de opiniones políticas.

La disposición legal a*d hoc* que establezca la base jurídica, en razón del interés público, para el tratamiento de estos datos especiales que son las opiniones de carácter político debería tener el máximo rango legal (es decir, una Ley Orgánica). Derechos y libertades fundamentales están implicados y, en consecuencia, se exigen las máximas garantías constitucionales e institucionales posibles, para preservar los derechos y el funcionamiento democrático. La(s) medida(s) legislativa(s) deberían recoger todos los extremos que señala el artículo 23.2 o el artículo 6, más arriba reproducidos, y otros factores que ha contemplado la doctrina (véanse las notas a pie de página números 33 y 35). Esa disposición podría limitar los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática. Medidas que limitan los derechos del Reglamento, y límites que deben ser conforme a los principios que el Tribunal de Derechos Humanos de Estrasburgo ha dispuesto en su jurisprudencia, en la cual sienta los principios que las leyes que regulan el tratamiento de datos *en interés público* deben cumplir.[34]

Los mecanismos para asegurar la transparencia deben ser claros y facilitar la información[35] necesaria para que el ciudadano sea consciente de la situación de su derecho a la protección de datos personales en determinados servicios y productos.[36] Por ejemplo, ser informado de si el perfil que se ha realizado lo ha sido mediante datos que ha hecho manifiestamente públicos el ciudadano (art.9.2.e) o si se han tomado de otras fuentes públicas (art.14.2.f).Transparencia que, en una sociedad democrática, es crítica para que el ciudadano ejerza sus derechos. Puesto que, en aras de un supuesto *interés público*, los derechos de protección de datos personales pueden ser sacrificados, incluso si se contemplan todas las garantías. De ahí que se insista en que la salvedad introducida en el art.23.2.h) no se aplique, pues no informar al ciudadano de la vigilancia y tratamiento de sus opiniones porque perjudique al interés público supone una violación de sus derechos, especialmente de la privacidad y de la libertad de expresión.

Conclusiones

El Reglamento establece en varias disposiciones, en términos abiertos y laxos, la base jurídica del *interés público* para justificar excepciones y límites a la prohibición general de tratamiento de datos personales especiales, como son las opiniones políticas. Los partidos políticos pueden tratar opiniones políticas en actividades electorales, si lo exigiera el funcionamiento democrático. Y podrían valerse de esta Ley y de la tecnología para *reinventar* sus funciones democráticas. Ahora bien, deben estar advertidos de que la misma ley y la misma tecnología pueden pervertir su papel, si no se toman las máximas garantías legales y controles técnicos necesarios, a riesgo de convertirse en manipuladores de los estados de opinión o, en su caso, simples correas de transmisión de opiniones en Internet, que pudieran no corresponder con la auténtica voluntad popular. Sin olvidar que el *big data analytics* ofrece correlaciones pero no causas, y los partidos debieran indagar en los *porqués* para ofrecer a los ciudadanos políticas correctas que incluyan a todos sin discriminar. Todo ello podría tener un impacto en los procesos democráticos.

Medidas legales, técnicas y organizativas deben extremarse en las operaciones con datos políticos. La transparencia debe ser garantía previa y acompañar a todas las demás, puesto que algunos derechos fundamentales pueden ser sacrificados, a pesar de las medidas, en aras del interés público. Las razones de interés público deben abandonar el lenguaje

ambiguo, y ser establecidas en una granular concreción en cada supuesto. Y es que podría producirse una falta de coherencia entre la ley y su aplicación efectiva.

La realidad digital muestra que existen muchos elementos, movimientos, comportamientos, datos, en definitiva, en la Red, que, procesados debidamente por las muchas y potentes herramientas disponibles, son capaces de destilar todas las ideas y opiniones políticas del usuario. Podría, pues, incluirse como *opinión política* un amplio espectro de datos, muchos de carácter especial. Se requiere, por parte de la ley, de un acotamiento bien definido de qué son o qué se comprende como opiniones políticas para su uso por los partidos, con el fin de garantizar la seguridad jurídica. La excepción del *interés público* podría cubrir una gran variedad de posibilidades, como las decisiones automatizadas y la elaboración de perfiles sobre la base de esta categoría particular de datos.

La recopilación y tratamiento de opiniones políticas con fines electorales, sin el respeto a los derechos fundamentales, puede significar un suicidio institucional, empezando por los propios partidos políticos. Las personas físicas y jurídicas requieren de derechos básicos para su propia subsistencia en una sociedad democrática, como la privacidad, la cual puede verse seriamente atacada sin el respeto a los datos personales. Al amparo del ejercicio del artículo 20 de la CE, los partidos y sus miembros pueden llevar a cabo una ilimitada actividad comunicativa con finalidad electoral, tanto en las redes sociales como utilizando otros recursos en la Red, sin vulnerar la vigente Ley Electoral. Además, puede decirse, que la propaganda se ha liberado de los límites legales de la campaña electoral y puede manifestarse de muchas maneras, precisamente con la ayuda de los datos.

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos y por el que se deroga la Directiva 95/46/ce (Reglamento General de Protección de Datos).

[2] El derecho a la privacidad es un derecho fundamental que, junto con la libertad de información y expresión, es esencial para la democracia y para la existencia de otros derechos fundamentales: asociación, reunión, participación, etc. (Schwartz, 1995)

[3] La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales ha introducido el artículo 58bis en la Ley Orgánica 5/1985, de 19 de Junio, del Régimen Electoral General (modificada el 2/11/2016). Este artículo sigue la misma línea de imprecisión que el Reglamento Europeo y hay que hacerle las mismas críticas.

[4] Afirman los autores: *Radical diferencia entre libertad de los antiguos y la libertad de los modernos; ésta reclama la privacidad, la libertad individual; aquélla reclama la participación en los asuntos de la comunidad*.

[5] Paul Ohm se centra en *highlighting the difficulty of protecting the privacy of data subjects by anonymizing data*; Paul M. Schwartz & Daniel J. Solove, en *discussing identification of individuals from personally identifiable information found from data sources*; y Rebecca J. Rosen, *explaining the ease with which metadata can be matched with specific individuals*.

[6] Carta de los Derechos Fundamentales de la Unión Europea (2016/C202/02): artículos 7 y 8.

[7] Me refiero concretamente a los Estados Unidos de América, donde se han producido prácticas tan criticadas como las de la consultora *Cambridge Analytica*, o las denunciadas por el analista de la CIA Snowden. La posible manipulación del proceso electoral en las últimas elecciones en los Estados Unidos de América (2016), como consecuencia del tratamiento de datos tomados de Facebook, está siendo probada (*El País*, 26 de Marzo 2018).

[8] La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, con la colaboración de las TICs e Internet, ha supuesto, en este sentido, una gran *revolución* que podría ser muy positiva.

[9] Sentencia del Tribunal de Derechos Humanos de Estrasburgo, de 29 de Junio del 2006. Weber and Saravia v Germany, Application no. 54934/00, Judgment of 29 June 2006, §§78–79. Establece criterios para realizar el test de la norma. Criterios parecidos ha establecido el Tribunal de Justicia de la Unión Europea (Rallo Lombarte, 2017).

[10]

> *Based on that earlier research, this article identifies a number of common themes in all 13 countries and develops a descriptive framework for analysing and comparing national laws on surveillance and government access to data held by the private sector. A normative framework was also developed based on a series of factors that can be derived from the concept of 'rule of law', from constitutional principles, and from existing (although still evolving) international human rights jurisprudence*. p. 97.

[11] Con el fin de preservar la *genuina* voluntad popular, podrían ambos ejercer funciones de alerta constante de *falsos o manipulados estados de opinión*, consecuencia de dinámicas comunicativas de las nuevas tecnologías (redes sociales, algoritmos, *bots*, motores de búsqueda, perfiles falsos, noticias falsas, posverdad, etc.). Es decir, primero desenmascarar para después compartir información y crear puntos de vista comunes.

[12] Ley Orgánica 5/1985, de 19 de Junio, del Régimen Electoral General. Modificada el 2/11/2016.

[13] Ahí se describe y analiza (Rubio y Vela) las distintas herramientas comunicativas y de relación con el ciudadano del Parlamento abierto.

[14] Los autores defienden la necesidad de un *derecho de anonimato* de la persona.

[15] El *whistlerblower*, del caso *Cambridge Analytica*, llamó la atención sobre la financiación de algunos partidos en el Brexit del Reino Unido (Vid. *El País* de 26 de marzo).

[16] Sin embargo, no siempre es previsible. Cuando se utilizan datos a gran escala como en el *big data*, o para fines estadísticos o de investigación, la finalidad concreta de los datos o necesidades de tratamiento concretas que puedan surgir, no siempre son previsibles desde el principio. Luego, hay una imposibilidad de pedir consentimiento o informar previamente (incluso *a posteriori)* de cada operación al ciudadano. Arts. 156 y ss Reglamento: transparencia proactiva y posterior.

[17] El caso de *Cambridge Analytica* es un ejemplo de los usos de datos con estos fines y en colaboración con *Facebook*. Y parece que tuvo resultado en las elecciones norteamericanas o en el Brexit británico, sea con el conocimiento y permiso de la propia red social o bien mediante otra estrategia. Véase esta información en el NYTimes, de 19 de Marzo de 2018, en la sección de opinión: *Facebook's Surveillance Machine.* También en el periódico *El País* de 21 de Marzo de 2018: *La compañía que burló la intimidad de 50 millones de estadounidenses.*

[18] *in many instances, we will need to give up our quest to discover the cause of things, in return for accepting correlations…Big data helps answer what, not why, and often that's good enough*. p. 29 Asimismo, advierten de la posibilidad de que el Estado se convierta en el *gran hermano* utilizando el *big data*. p. 37.

Véase también el informe del MIT: Summary Report of *Big Data Privacy Workshop: Advancing the State of the Art in Technology and Practice* (MIT).

[19]

> *El proceso de reducción de la complejidad en un sistema democrático descansa en una multiplicidad de mecanismos, todos ellos necesarios en la medida en que facilitan la participación política como presupuesto del sistema. ….En primer lugar, los derechos informativos….un primer nivel de formación de la opinión pública…En segundo lugar, ..los partidos políticos que racionalizan la oferta electoral… Un tercer mecanismo de reducción de la complejidad es el sistema electoral como procedimiento…Y como último mecanismo… el Parlamento.* pp. 32-33

[20] Véase también la Conferencia de la NYU: Governing Algorithms. A Conference on Computation, Automation and Control". New York University. May 16, 2013.

[21]

> *Si tradicionalmente el Parlamento era el centro de la producción política y los medios de comunicación constituían su elemento de transmisión en nuestros días esa relación ha cambiado: la publicidad ya no es el objetivo de las actuaciones parlamentarias sino su premisa, y el desencadenante para que el Parlamento actúe. Hoy los ciudadanos prestan más atención a los hechos políticos publicados que [a](sic)los debatidos en el Parlamento*. p. 109.

[22] El autor diferencia entre la *classical conception of propaganda* y *propaganda as biased speech*. Y diferencia la propangada que se realiza en los países totalitarios de la que llevan a cabo las democracias liberales: I*t is only natural in liberal democratic societies to take at least the news media seriously. The problem in democratic societies lies in figuring out which apparently non propangandistic claims are in fact propaganda*, p. 46. Esta confusión se acrecienta en la Red.

[23] En las Instrucciones del Junta Electoral Central (citadas en el texto), así como en su doctrina, en un intento de adaptar la Ley General Electoral a los nuevos medios electrónicos, se diferencia entre cuentas públicas (institucionales) y privadas en las redes sociales. Cuando se

utilizan las institucionales, por el Gobierno o Poderes Públicos, en periodo electoral, está prohibido en virtud del principio de neutralidad que deben mantener durante todo el periodo electoral. Pero si se trata de cuentas privadas de los candidatos, no habría ninguna limitación, en virtud del derecho a la libertad de expresión. En cuanto a otros medios electrónicos, el criterio de prohibición viene dado por la *contratación comercial*, ya sea en redes, plataformas, webs, etc… de espacios o contenidos electorales fuera del tiempo de la campaña electoral.

[24] La investigación científica del perfilado psicológico usando datos sociales valida que se puede perfilar a las personas por atributos psicológicos y explotar esa información.

[25] Vid. web de la Junta Electoral Central.

[26] El analista informático de la Consultora *Cambridge Analytica* Christopher Wylie declaraba a la prensa:

> *La diferencia es cuando engañas, cuando creas una realidad a medida para alguien, cuando te diriges a alguien porque sabes que es más susceptible de entrar en teorías conspiratorias porque lo has perfilado así, y lo llevas a una espiral de noticias falsas. Es diferente a llamar a una puerta determinada identificándote como parte de una campaña. Una de las cosas que hacíamos en Estados Unidos es investigar esa noción del deep state y la paranoia con el Gobierno. Cosas como qué pasa si vienen y se llevan tus armas. Puedes perfilar a un grupo de personas muy receptivas a esas teorías conspiratorias, del tipo de que Obama ha desplazado tropas a Texas porque no está dispuesto a irse. Entonces fabricas blogs o webs que parecen noticias y las muestras todo el tiempo a la gente más receptiva a ese pensamiento conspiratorio. Después ven la CNN y no hay nada de lo que ven todo el tiempo en Internet, y piensan que la CNN esconde algo.* (*El País,* 26 de Marzo 2018).

[27] Considerandos (50) y (51) del Reglamento.

[28] El Reglamento dice tajantemente en el art. 9.2. *e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;*

[29] Véase el considerando 85:

> *Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, ….*

[30]

> *..in every country studied, even those nations with otherwise comprehensive data protection laws, access for regulatory, law enforcement, and national security purposes is often excluded*

> *from such laws; alternatively, they are treated as accepted purposes for which access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses. Moreover, almost everywhere, when it comes to data protection access for national security purposes is more sparingly regulated than is access for law enforcement purposes.* p.97.

[31] Considerandos del Reglamento: 47 y ss; 51, 50, 52, 53, 54, 55, 56, y 73 final. Artículos 2, 6 y en relación con los arts. 6.2, 6.4, 23 y 89. Se reproduce a continuación los considerandos 69 y 65:

> *(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada e**n interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero**, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento ….*
>
> *(65) Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de **una misión realizada en interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento, **por razones de interés público** en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica …*

[32] Los factores que Rubistenin y los otros coautores entienden que deben contener las garantías de estas limitaciones, hechas en razón del interés público o intereses generales son:

> *Assessing surveillance laws under Article 8, 14, normative factors should be considered in evaluating laws for systematic access: 1. In accordance with law—… 2. Court order—… 3. Approval of senior official… 4.Limited to serious crimes or serious threats—… 5. Particularity as to target—… 6. Showing of suspicion—… 7. Exhaustion of less intrusive means—… 8. Limit on duration—… 9. Limit on scope ('minimization' of irrelevant data)—… 10. Limit on use and disclosure—… 11. Retention limit/limit on storage—… 12. Notice to target—… 13. Oversight by independent entity—… 14. Redress —….*

[33] Vid. Web de la Agencia Española de Protección de Datos.

[34] Se ha citado en nota núm. 8.

[35] Considerando del Reglamento (62):

> *Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas*.

[36]

> *A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes* (Considerando 100 del Reglamento).

Bibliografía

AGEPD. (2018). Guía para Responsables del Tratamiento 29-5-2018. Disponible en: http://www.agpd.es/portalwebagpd/index-ides-idphp.php (consultado el 8 de febrero de 2019).

APARICIO PÉREZ, M. y BARCELÓ I SERRAMALERA, M. (2009). *Manual de Derecho Constitucional.* Barcelona: Atelier.

ARANDA ÁLVAREZ, E. (2017). "Parlamento abierto: una visión desde los principios de funcionamiento de las cámaras parlamentarias". *Revista Española de Derecho Constitucional,* 111, 13-43.

CUKIER, KENNETH, C. and MAYER-SCHOENBERGER, V. (2013). *Big Data: A Revolution That will Transform How We Live, Work and Think*. N.Y.: Houghton Mifflin Harcout.

FERNÁNDEZ MIRANDA, C., Y FERNÁNDEZ MIRANDA, A. (2003). *Sistema electoral, Partidos políticos y Parlamento*. Madrid: Editorial Colex.

GARCÍA SANZ, R.M. (1990). *El derecho a opinar libremente.* Madrid: Editorial Eudema.

GARCÍA SANZ, R.M. (2017). *Digital Journalism. Rethinking Communication Law to Support Democracy and Viable Business Models.* Palo Alto: Academica Press.

GUIMÓN, P. (2018). "El Brexit no habría sucedido sin Cambridge Analytica". *El País*. 26 -3-2018. Disponible en: www.elpais.com (consultado el 8 de febrero de 2019).

JASON, S. (2015). *How Propaganda Works,* N.J.: Princeton University.

Junta Electoral Central. (2018). Instrucciones.
Disponible en: http://www.juntaelectoralcentral.es/cs/jec/doctrina/instrucciones (consultado el 8 de febrero de 2019).

KOSINSKI, M., STILLWELL, D. Y GRAEPEL, T. (2013). "Private traits and attributes -are predictable from digital records of human behavior". *PNAS* , 110 (15), 5802-5805.
Disponible en: https://doi.org/10.1073/pnas.1218772110 (consultado el 8 de febrero de 2019).

MARTIN, J.A. Y FARGO, A.L. (2015). "Anonymity as a Legal Right: Where and Why It Matters". *N.C. J.L. & Tech*., 16, 311-375.

MARTINEZ AHRENS, J. (2018). La compañía que burló la intimidad de 50 millones de estadounidenses. *El País,* 21-3- 2018.
Disponible en: www.elpais.com (consultado el 8 de febrero de 2019).

MIT. (2014). Summary Report of Big Data Privacy Workshop: Advancing the State of the Art in Technology and Practice.
Disponible en :
http://web.mit.edu/bigdata-priv/images/MITBigDataPrivacyWorkshop2014_final05142014.pdf (consultado el 8 de febrero de 2019).

NISSEBAUM, H, y BAROCAS, S. (2014). "Big Data's End Run around Anonymity and Consent". En LANE, J. et al. (Editors). *Privacy, Big Data, and The Public Good: Frameworks for Engagement.* (pp. 44-76). N.Y: Cambridge University Press.

NYU School of Law. (2013). Governing Algorithms. A Conference on Computation, Automation, and Control. New York University. May 16, 2013.
Disponible en: http://governingalgorithms.org#govalgo (consultado: 9 de Mayo 2018).

OHM, P. (2010). "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". *UCLA L. Rev.*, 57, 1701-1759.

RALLO LOMBARTE, A. (2017). "El Tribunal de Justicia de la Unión Europea como Juez Garante ----------de la Privacidad en Internet". *Teoría y Realidad Constitucional,* 39, 583-610.

REITINGER, N. (2015/2016). "Algorithmic Choice and Superior Responsibility: Closing the Gap Between Liability and Lethal Autonomy by defining the Line Between Actors and Tools". *Gonz.L. Rev.,* 51, 79-118.

ROSEN, R.J. (2013). "Stanford Researchers: It Is Trivially Easy to Match Metadata to Real People". *Atlantic,* 24-12-2013.
Disponible: http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-realpeople/282642/ http://perma.cc/QFK5-6JUC

RUBINSTEIN, I.S., NOJEIM, G.T. y LEE, R.D. (2014). "Systematic government access to personal data: a comparative analysis". I*nternational Data Privacy Law,* 4, (2), 96-119.

RUBIO NÚÑEZ, R. y VELA NAVARRO-RUBIO, R. (2017a). *Parlamento Abierto. El Parlamento en el Siglo XXI*. Barcelona: Editorial UOC

RUBIO NÚÑEZ, R. Y VELA NAVARRO-RUBIO, R. (2017b). *El Parlamento Abierto en el Mundo, Evolución y Buenas Prácticas.* Zaragoza: Fundación Manuel Giménez Abad.

RUBIO NÚÑEZ, R., (coord.). (2014). *Parlamentos abiertos. Tecnología y redes para la democracia.* Madrid: Congreso de los Diputados.

SÁINZ MORENO, F. (1976). *Conceptos jurídicos indeterminados, interpretación y discrecionalidad administrativa*, Madrid: Editorial Civitas.

SCHWARTZ, P. (1995). "Privacy and Participation: Personal Information and Public Sector Regulation in the United States". *Iowa L. Rev.*, 80, 557-618.

SCHWARTZ, P., & SOLOVE, D.J. (2011). "The PII Problem: Privacy and a New Concept of Personally Identifiable Information". *N.Y.U. L. Rev.*, 86, 1814-1894.

TUFEKCI, Z. (2018). "Facebook's Surveillance Machine". *New York Times,* 19 -3- 2018. Disponible: www.nytimes.com (consultado el 8 de febrero de 2019).

WEBER, S y WONG, R.Y. (2017). "The new world of data: Four provocations on the Internet of Things". First Monday. Peer-Reviewed Journal on the Internet, 22 (2).
Disponible: http://dx.doi.org/10.5210/fm.v22i2.6936.