

TRATAMIENTO DE DATOS PERSONALES DE LAS OPINIONES POLÍTICAS EN EL MARCO ELECTORAL: TODO EN INTERÉS PÚBLICO¹

Processing personal political opinion data in electoral
activities: all in the public interest

ROSA MARÍA GARCÍA SANZ

Universidad Complutense de Madrid

rosamaga@pdi.ucm.es

Cómo citar/Citation

García Sanz, R. M. (2019).

Tratamiento de datos personales de las opiniones políticas
en el marco electoral: todo en interés público.

Revista de Estudios Políticos, 183, 129-159.

doi: <https://doi.org/10.18042/cepc/rep.183.05>

Resumen

El Reglamento de Protección de Datos pone a disposición de los partidos políticos numerosas disposiciones que establecen el «interés público» como base jurídica para el tratamiento de datos personales en actividades electorales. En aras del interés público, pueden tratar datos sensibles, como son las opiniones políticas, limitando seriamente los derechos y principios de la persona titular del derecho fundamental, si se entiende que así lo exige el funcionamiento democrático.

Palabras clave

Protección de datos personales; actividades electorales; tratamiento de opiniones políticas.

¹ Este artículo es consecuencia de mi estancia de investigación en la Berkeley Law School (BCLT 2017).

Abstract

The General Data Protection Regulation (GDPR) includes several provisions that allow political parties to lawfully process political opinion data based on the “public interest” during electoral activities. As the operation of democratic systems in Member States motivates political parties to compile data on citizens’ political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established. However, it is argued that the fundamental right of personal data protection can be seriously limited, or even ignored, in such circumstances.

Keywords

Personal data protection right; electoral activities; political opinions processing; privacy.

SUMARIO

I. INTRODUCCIÓN. II. IDENTIFICANDO EL «INTERÉS PÚBLICO» EN EL REGLAMENTO: INDAGACIÓN DE LAS RAZONES DEL LEGISLADOR: 1. Razones del legislador: la crisis de los intermediarios democráticos. 2. Localización en el Reglamento: detectando riesgos y oportunidades: 2.1. *La prohibición general del tratamiento de datos sensibles de opinión política: su excepción por interés público.* 2.2. *La habilitación legal del interés público para tratar los datos sensibles de las opiniones políticas por los partidos políticos en el marco de actividades electorales.* III. «INTERÉS PÚBLICO»: UN CONCEPTO JURÍDICO INDETERMINADO PARA LIMITAR (Y POSIBLEMENTE DESNATURALIZAR) EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS: 1. Midiendo los límites al derecho a la protección de datos personales: 1.1. *Base jurídica.* 1.2. *Finalidad.* 1.3. *Sujetos.* 1.4. *Objeto.* 1.5. *Tiempo.* 1.6. *Espacio.* 1.7. *Contenido.* 2. Aparente conflicto de derechos fundamentales: una perspectiva desde su dimensión institucional. IV. CONCLUSIONES. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

El objeto de este trabajo es el análisis y la reflexión de las disposiciones del Reglamento² dirigidas al tratamiento de datos personales de las opiniones políticas, autorizados los partidos políticos por razones de «interés público», si así lo «exige el funcionamiento democrático», y en el «marco de actividades electorales». Identificar «qué» interés público es necesario atender para que «funcione el sistema democrático» en este contexto es uno de los aspectos principales de este estudio. Pues ese interés público justificaría la batería de límites al derecho fundamental de protección de datos personales por parte de los partidos, hasta el punto de desnaturalizarlo. Se concluirá que las razones de interés público deberían ser la identificación y/o formación de la voluntad popular, que se puede ver falseada debido a los fenómenos de desinformación y manipulación de datos en los medios electrónicos. Esta finalidad justificaría los límites previstos. Ahora bien, tal autorización legal no está exenta de graves riesgos. Por lo cual, entiendo que solo debería habilitarse a los partidos en situaciones de absoluta certeza de

² 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).

injerencia o manipulación de la opinión pública y tiempo muy acotado; y la utilización de los límites disponibles por «interés público», bajo criterio muy restrictivo.

Esta situación de «presunta» excepcionalidad democrática impacta el contenido esencial del derecho, dando, aparentemente, preferencia al derecho fundamental de participación política en la tensión de derechos, y sin ignorar potenciales consecuencias en otros derechos fundamentales. Situación de excepcionalidad que podría asociarse con la que sufre el derecho a la información en campaña electoral, con restricción intensa de su contenido. Sin embargo, no es comparable. Primero, porque tales medidas restrictivas de la legislación electoral sobre los medios de comunicación ya han mostrado su inoperancia en los soportes electrónicos. Y segundo, porque la naturaleza del derecho a la protección de datos personales es diferente, y su impacto en otros derechos fundamentales es de tal magnitud que no solo dejaría sin sentido al derecho de sufragio, sino, también, a otros derechos fundamentales necesarios en el proceso democrático. Y tampoco se parece al régimen de excepcionalidad reconocido a los partidos para el tratamiento de las opiniones políticas de sus miembros, en el ámbito de su organización (art.9.2.d), que es excepcional pero en la normalidad democrática. Aspectos estos que ya han sido tratados por la doctrina, pero, desde la perspectiva de las disipaciones del Reglamento objeto de estudio, muestran nuevas problemáticas.

El legislador europeo no solo introduce un «concepto jurídico indeterminado» (interés público) para legitimar el tratamiento de los datos personales de las opiniones políticas de las personas, sino que, también, los términos que lo acompañan, tanto en el considerando 56 como en los artículos con los que se relaciona en el Reglamento, son laxos y abiertos. Así, al riesgo de discrecionalidad y arbitrariedad que se puede derivar de la interpretación de «interés público», se suma la imprecisión de términos como «en el marco de actividades electorales», «opiniones políticas de las personas» o si «el funcionamiento democrático lo exige», todos ellos igualmente poco precisos y expresados con gran amplitud (sobre todo si se piensan en la realidad digital). Tanto indeterminación e imprecisión llama la atención en un asunto de tanta importancia, donde confluyen distintos derechos fundamentales. Derechos fundamentales necesarios para el funcionamiento democrático, especialmente el derecho a la privacidad o el derecho de sufragio, sin olvidar el derecho a la libertad ideológica o el derecho a la libertad de expresión e información. En esta confluencia de derechos, destaca la tensión entre el derecho a la protección de datos personales y el derecho de participación: parece, en principio, que el legislador opta por la limitación del primero —y probablemente su desnaturalización—, utilizando el interés público para dar prioridad y expansión al derecho de participación. Ahora bien, dado que los conceptos jurídicos indeterminados van a

exigir una toma de posición del legislador, introduciendo el inevitable sesgo ideológico, desde la dimensión institucional se puede considerar una delimitación de estos derechos (para hacer que funcione el sistema) que viene exigida por los profundos cambios producidos por la tecnología de la información, con consecuencias políticas, sociales y económicas. Ello requerirá observar si tal operación respeta el contenido esencial de los derechos fundamentales en su dimensión subjetiva, y si las intromisiones se justifican material y temporalmente. Estas acciones tienen un adecuado acomodo en un Estado social y democrático de derecho, que exige a los poderes públicos una acción de promoción de condiciones y remoción de obstáculos (art. 9.2 CE) para el ejercicio real e igual de los derechos fundamentales. Y, en el contexto del constitucionalismo democrático, corresponde, en primer lugar, al legislador determinar los criterios de ponderación de derechos e intereses públicos en conflicto.

El Reglamento, aunque de aplicación directa, hace una llamada al legislador de los Estados miembros y da margen de interpretación en la norma de adaptación. Ahora bien, el Reglamento ya ha establecido los términos básicos. En principio, la expectativa de una legislación con parámetros legales precisos, capaz de ofrecer seguridad jurídica a las prácticas que utilizan datos personales con fines de electorales, se ha visto frustrada³. Lejos de ofrecer seguridad, el Reglamento presenta una mayor incertidumbre, y podría dar, irónicamente, cobertura legal incluso a prácticas poco respetuosas, en virtud de sus conceptos jurídicos indeterminados y vagos. España, siguiendo la misma línea del Reglamento europeo, con términos ambiguos y conceptos jurídicos indeterminados, ha incorporado el art. 58 bis —introducido por la disposición final tercera de la Ley Orgánica que adapta el Reglamento⁴— a la Ley Orgánica del

³ Muestra de ello es el paquete de medidas anunciadas por el presidente de la Comisión Europea en el discurso del Estado de la Unión de 2018, el 12 de septiembre: <http://bit.ly/2HFfjNH>. Destacamos: las Orientaciones de la Comisión sobre la aplicación de la legislación de protección de datos de la Unión en el contexto electoral; la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE, Euratom) núm. 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, Bruselas, 12-9-2018 COM(2018) 636 final, y la Recomendación de la Comisión sobre las redes de cooperación electoral, la transparencia en línea, la protección contra incidentes de ciberseguridad y la lucha contra las campañas de desinformación en el contexto de las elecciones al Parlamento Europeo, Bruselas, 12-9-2018 C(2018) 5949 final.

⁴ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Régimen Electoral General (LOREG)⁵. Este artículo viene a autorizar la recopilación de datos personales de las opiniones políticas en el marco electoral por los partidos políticos. El Reglamento, de aplicación directa, no arrojará mucha luz para aclarar el nuevo art. 58, pues se producirá, presumiblemente, un círculo vicioso de indeterminación e inseguridad jurídica: el Reglamento llama a la ley específica para su concreción y esta no encontrará mayor precisión en el Reglamento. Tampoco la LOREG ayudará mucho, pues ni su espíritu ni su letra responden al mundo digital, y el propio art. 41 prevé que los partidos reciban información disociada de los datos.

El punto de partida de este trabajo arranca de lo ya sentado por la doctrina respecto a los riesgos que conllevan las nuevas tecnologías en el tratamiento de datos personales durante el período electoral (Rubio, 2011: 319); o del impacto de estos tratamientos en los principios jurídicos de la campaña electoral y en los derechos de participación (García Mahamut, 2015: 309-338). Los principios electorales se han «truncado» por la incorporación de los nuevos medios electrónicos en el proceso electoral, produciéndose *de facto* ventaja competitiva y afectando al juego limpio democrático (*ibid.*: 328 y ss.). Asimismo, más de una voz se ha alzado ya advirtiendo de la obsolescencia de la legislación electoral, especialmente la española, y advirtiendo de sus consecuencias (Holgado González, 2017: 457-485). El uso de Internet y todas sus herramientas sobrepasa todas las previsiones de las normas electorales vigentes en materia de datos personales (normativa parca, a excepción de la del censo electoral) e incluso supera en muchas ocasiones la normativa general de protección de datos personales (muchas herramientas en la Red requieren y tratan datos personales para su solo funcionamiento técnico, ajenas a las normativas). La multiplicidad de herramientas tecnológicas conlleva la posible captación sin consentimiento de datos personales, que, usados en estrategias electorales personalizadas y masivas, desafían las normas y sus garantías. Para subrayar la trascendencia de las disposiciones del Reglamento, hay que ponerlas en este contexto y preguntarse si dan solución a la problemática. Cabe añadir que la rápida evolución y los cambios de la tecnología digital, a ritmo incesante, solo han hecho que aumentar y exacerbar muchas de las situaciones de riesgo que la doctrina ha detectado, y que aquí se intentan recoger para completar aquella visión. Pero aún más: si no se acotan afiladamente los términos del considerando 56 relacionado con las pertinentes disposiciones del Reglamento, las muchas y amplias limitaciones «por interés público» podrían empeorar las cosas.

⁵ Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, modificada el 2-11-2016.

En el trabajo se siguen estos pasos. En el segundo epígrafe, se indagarán las razones que el legislador de la Unión pudo prever para que el sistema democrático pueda exigir, por «interés público», el tratamiento de estos datos personales. Seguidamente, se localizarán las disposiciones del Reglamento en las que se recurre al «interés público». Con la muestra, no exhaustiva pero suficiente, se pretende conocer la dimensión que podría alcanzar la habilitación legal de tratar datos personales de las opiniones políticas por los partidos en el marco electoral, y las posibles restricciones al derecho, en sistemática con el resto del Reglamento. En el tercer epígrafe se analiza la intensa restricción que podría sufrir el derecho de protección de datos. Limitación que parece justificarse para dar preferencia al derecho de participación política y favorecer el funcionamiento democrático. Se afrontará, entonces, el posible conflicto de derechos, para observar que, si no se acotan muy bien los elementos para establecer los límites del primer derecho, no solo se puede producir una desnaturalización del primero sino también del segundo. Pues si el objetivo es expansionar el derecho de participación, a expensas del derecho de datos personales, podría producirse una perversión: la invasión de la privacidad de las personas serviría para desnaturalizar el derecho de sufragio. Es decir, que el sufragio, que el art. 68 CE exige que sea libre, secreto, igual y directo, dejaría de serlo a consecuencia de la injerencia en los datos y en la privacidad de la persona; dado que con la ayuda de sofisticadas herramientas —algoritmos o inteligencia artificial— se puede, más que predecir, determinar el voto de cada elector (Rubio, 2011: 329). Habría que concluir, si se procede de esta manera, que la habilitación no serviría para la formación de la opinión pública, con el fin del funcionamiento democrático.

II. IDENTIFICANDO EL «INTERÉS PÚBLICO» EN EL REGLAMENTO: INDAGACIÓN DE LAS RAZONES DEL LEGISLADOR

El legislador europeo ha identificado una situación donde el «interés público» parece justificar, cuando menos, una limitación de derechos fundamentales. Las dificultades que presenta un «concepto jurídico indeterminado» como el «interés público» no son algo nuevo. La complejidad del problema ya ha sido tratada extensamente por la doctrina (véase, por todos, Sáinz Moreno, 1976), por lo tanto, solo cabe aquí intentar aprovechar los recursos que allí se ofrecen tanto desde el ámbito administrativo como en el de la esfera del legislativo y en sede judicial para su control por los tribunales. Como indica López Calera (2010: 147):

La indeterminación del concepto nunca podrá ser salvada en términos absolutos. Sólo la «democraticidad» de su constitución y de su realización puede ser la

garantía más eficaz para evitar los desmanes que puede producir su indeterminación. El poder legislativo, que es el poder más legitimado democráticamente, es el primer responsable de ubicar con razones, y con la precisión posible, el interés público en los contenidos materiales de las normas jurídicas. El poder legislativo tiene esa máxima discrecionalidad para realizar tal función dentro de los límites de la Constitución.

En este sentido, el legislador europeo, explícita o implícitamente, manifiesta en el Reglamento unas razones, y remite a medidas legislativas posteriores del derecho de la Unión o de los Estados miembros (art. 6.3) para especificar las razones concretas que llenen de contenido la base jurídica del «interés público» invocada, que autoriza a los partidos a tratar datos personales sensibles en relación con las opiniones políticas para «el funcionamiento democrático». En definitiva, será en la norma que detalle los elementos y circunstancias de la situación concreta donde se pueda especificar qué y por qué se satisface un interés general para el funcionamiento democrático. Advertidos de que el fin del «interés público», junto con otros fines que explican Rubinstein *et al.* (2014: 1 y ss.), como la seguridad nacional, la seguridad pública, la lucha contra el terrorismo, el cumplimiento de las normas, razones administrativas o razones democráticas, etc., se repiten tanto en las leyes de protección de datos como en aquellas extramuros de estas, 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 (*ibid.*: 97). 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 (*ibid.*: 98).

1. RAZONES DEL LEGISLADOR: LA CRISIS DE LOS INTERMEDIARIOS DEMOCRÁTICOS

El legislador europeo no es ajeno a los problemas de las democracias de la Unión, causados, entre otras razones, por el impacto que los nuevos medios de comunicación electrónicos han provocado en su funcionamiento,

especialmente en el período electoral (las citadas medidas de la Comisión lo prueban). La comunicación política y la campaña electoral se han trasladado de los medios de comunicación convencionales a los novísimos espacios de Internet, desafiando las normas electorales y las propias reglas de juego democrático.

Los principales actores de la batalla electoral —partidos políticos y medios de comunicación— se han visto profundamente afectados por tal transformación. Y no solo durante el período electoral, sino permanentemente en su función de formación de la opinión pública. Función que se exacerba durante el tiempo de campaña. La crisis de los intermediarios en la participación política —partidos y medios de comunicación— supone también la crisis de la formación de la opinión pública, con consecuencias jurídico-políticas importantes (Bustos Gisbert, 2017: cap. III). Se aboga por mejorar los mecanismos de la formación de la opinión pública, y, posiblemente, el legislador europeo ha querido aquí introducir un mecanismo al servicio de los partidos políticos.

Cabe pensar que el proceso de formación de la llamada opinión pública, a través de los espacios electrónicos, mediante una comunicación pública libre, en la que todos pueden hacer oír su voz directa, legítimamente y sin filtros, es más genuino que nunca, y en las mejores condiciones para expresar el pluralismo político. Sin embargo, fenómenos de desinformación (*fake news*, posverdad), acceso y manipulación de datos personales sin consentimiento (caso *Cambridge Analytica*)⁶, falsas cuentas en las redes, la utilización de *bots*, *trolls*, falsa viralización de mensajes por el uso de algoritmos e inteligencia artificial —nombrando solo algunos— han provocado manipulación, confusión y falsificación de la opinión pública, cuya centralidad en el funcionamiento democrático está fuera de dudas. Las disposiciones del Reglamento introducirían así un mecanismo legal para que los partidos (en colaboración con otros agentes)⁷

⁶ El caso *Cambridge Analytica* es un ejemplo, y en colaboración con Facebook. Véase esta información en el *NYTimes*, de 19 de marzo 2018, en la sección de opinión: «Facebook's Surveillance Machine». Y para la posición de la UE ante este escándalo, véase la Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos (2018/2855(RSP)).

⁷ Recomendación de la Comisión de 12-9-2018, citada anteriormente. Se anima a los Estados miembros a que creen una red nacional de cooperación electoral integrada por las autoridades pertinentes —como las autoridades electorales, de ciberseguridad, de protección de datos y policiales—, y a que designen un punto de contacto para que participen en una red de cooperación electoral a nivel europeo. También la resolución del Parlamento citada, en el punto 11, considera que «la injerencia en las elecciones

puedan desenmascarar los falsos estados de opinión, identificando si las opiniones políticas son consecuencia del libre ejercicio de la libertad de expresión e información de las personas (sus datos personales) o si, por el contrario, han sido falseadas, o los estados de opinión, manipulados. La clásica función de los partidos de reducir la complejidad (Fernández Miranda y Fernández Miranda, 2003: 32-33)⁸ en un sistema democrático, que podría haberse visto comprometida en principio (por la fragmentación, dispersión y burbujas de opinión en la Red), podría reafirmarse de nuevo, finalmente, si los partidos se reinventan aprovechando las posibilidades del Reglamento.

En situaciones en las que la auténtica voluntad popular esté siendo amenazada, y haya fundadas sospechas o evidencias suficientes, es razonable afirmar que el sistema democrático requiere de tal autorización para que los partidos accedan a los datos personales, conozcan quién está detrás e identifiquen a la auténtica «opinión pública», y puedan llevar a cabo su acción electoral.

Hay recordar que los medios de comunicación institucionalizados han dejado de ser el canal exclusivo de comunicación entre los ciudadanos, los partidos políticos y los representantes parlamentarios. Los partidos tampoco ya son el instrumento exclusivo para la participación política. El ciudadano prefiere comunicarse directamente por los medios electrónicos para ejercer sus derechos de expresión y participación, prescindiendo de ambos intermediarios, debido a la crisis de confianza que medios convencionales y partidos sufren por cuenta propia (García Sanz, 2017). Igualmente, los políticos prefieren relación directa con el ciudadano y potencial elector. La tradicional formación de la llamada opinión pública —concepto igualmente indeterminado— por los medios de comunicación institucionalizados se ha realizado mediante la producción de mensajes que, para merecer la protección constitucional, debían responder al «interés público» y cumplir con los requisitos constitucionales⁹. De esta manera, el ejercicio del derecho a la información se ha considerado garantía institucional de la formación de opinión pública libre, necesaria para expresar el pluralismo político-social. De esta garantía carecen espacios de comunicación electrónicos

constituye un importante reto para la democracia, y para combatirla se requiere el esfuerzo conjunto de los proveedores de servicios, los reguladores y los agentes y partidos políticos».

⁸ «El proceso de reducción de la complejidad en un sistema democrático descansa en una multiplicidad de mecanismos [...]. 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).

⁹ Por todas: STC 171/90.

como las redes sociales. Los medios convencionales han servido tradicionalmente a los partidos y a las instituciones para identificar el «interés general» de la ciudadanía. Se ha entrado así en una crisis en la formación de la opinión pública e, igualmente, en una crisis de la identificación de los intereses generales para que los partidos cumplan sus funciones. Crisis de conceptos indeterminados que se complica en la Red (Torres del Moral, 2013: 1383 y ss.).

Los intereses generales pueden estar muy fraccionados, manipulados, y la opinión pública, falseada. El pluralismo político, principio estructural democrático, tiene una relevancia institucional indiscutible. Pero ese pluralismo político puede estar falseado con una manipulación de los datos en la Red. Cuando accedan a los estados de opinión, los partidos deben estar advertidos de las anomalías que se producen en Internet. Fenómenos de desinformación, unidos a otros de no menor importancia (como la *filter bubble* o la *echo chamber* y la utilización de algoritmos con datos a gran escala, que permiten tratar informativamente a los usuarios por sus perfiles psicoideológicos), corrompen la llamada «opinión pública», y, en consecuencia, el proceso electoral y el sistema representativo. A su vez, los partidos, para identificar datos, opiniones e intereses, cuentan con muchas herramientas: algoritmos e inteligencia artificial para crear categorías. Sin embargo, todas estas técnicas no están exentas de riesgos: el análisis que se realiza del *big data* ofrece correlaciones, no causas (Cukier y Mayer-Schoenberger, 2013: 29, 37), y la toma de decisiones para el interés general requiere saber los «porqués» para ofrecer políticas y legislaciones correctas que incluyan a todos sin discriminar. Y la inteligencia artificial y los algoritmos pueden contener sesgos, enfocando los resultados hacia una dirección predeterminada.

El legislador de la Unión tiene, en principio, una buena razón: dar soluciones, en los términos del Reglamento, con mejor o peor fortuna, a la problemática de la identificación y/o formación de la opinión pública, y de los intereses generales, en una democracia que ya es digital (Rubio Núñez y Vela Navarro, 2017a).

Ahora bien, la doctrina debe ahondar sobre los conceptos de «opinión pública¹⁰» y «pluralismo político» en el contexto digital. Si las redes son la opinión pública misma (identificable por sus datos, público opinante) expresando el pluralismo político; o si el conjunto de opiniones políticas publicadas en los espacios digitales (y no digitales), expresando diferentes intereses, en el ejercicio del derecho a la información, conformará después la opinión pública.

¹⁰ Si solo las opiniones publicadas o manifestadas públicamente, o también manifestadas en privado pero en espacios públicos (Weber y Wong, 2017), y si extraídas tanto de los medios convencionales como de las redes sociales, blogs, buscadores, etc.

El proceso de su formación es susceptible de interpretaciones diferentes. El Tribunal Constitucional ha mantenido en numerosa jurisprudencia¹¹ que el ejercicio de las libertades del art. 20 CE es la garantía institucional de la opinión pública libre, que después manifiesta el pluralismo político. Sin embargo, siguiendo una interpretación doctrinal distinta (Bastida, 1994: 11; Villaverde, 1994: 299), puede producirse un cambio de paradigma: si se interpreta que es la opinión pública misma expresando el pluralismo político y social en los espacios electrónicos. Se colocaría a los partidos en una posición diferente en cuanto a su función de formadores de la opinión pública.

2. LOCALIZACIÓN EN EL REGLAMENTO: DETECTANDO RIESGOS Y OPORTUNIDADES

En este apartado se van a identificar «considerandos» y artículos significativos en los que la base jurídica del «interés público» (art. 6.1.e) y las excepciones por interés público pueden servir a los partidos políticos con el objetivo descrito en el considerando 56. Se reproducirán algunos de ellos, y se acompañarán comentarios al hilo de su lectura, sugeridos por algunos aspectos preocupantes de los posibles límites. El Reglamento, tanto en su art. 2.1.d), por el ámbito de aplicación material¹², como en distintos artículos, introduce esa finalidad ya identificada de «interés público». Los riesgos (y oportunidades) que pudieran derivarse no solo afectan al propio país sino incluso más allá de la propia UE (art. 2.1.a), por la naturaleza global de Internet¹³. En el apartado siguiente se concretarán las posibles restricciones que pueden «desnaturalizar» el contenido esencial del derecho. El conjunto de disposiciones objeto de estudio se encabeza por el considerando 56:

Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos

¹¹ Son innumerables, pero véase por todas: STC 6/1981.

¹² Dictamen del Consejo de Estado de 26 de octubre de 2017, relativo al Anteproyecto de Ley Orgánica de Protección de Datos de carácter Personal: «[La] aplicabilidad supletoria del Reglamento Europeo, en los casos en principio no sometidos al Derecho de la Unión, lleva consigo la de la jurisprudencia interpretativa del mismo, así como la competencia prejudicial del Tribunal de Justicia (STJCE de 18 de octubre de 1990, *Dzodzi*, asuntos acumulados C-297/88 y C-197/89)».

¹³ La citada resolución del Parlamento Europeo sobre el caso *Cambridge Analytica* dice en su punto 28: «A la luz de la confirmación por parte de Facebook de que se han producido graves violaciones de la privacidad, pide a las autoridades de los Estados Unidos responsables de la aplicación del Escudo de la Privacidad que reaccionen [...]».

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 permite un ámbito de tratamiento de datos personales de las opiniones políticas por parte de los partidos políticos que podría dañar los derechos fundamentales¹⁴ de los ciudadanos en aras, supuestamente, de la democracia representativa y participativa (Fernández Miranda y Fernández Miranda, 2003: 25)¹⁵. 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: 1877-1878; Rosen, 2013)¹⁶ y la reidentificación es posible siempre (Nissenbaum y Barocas, 20014: 49-50). La facilidad con la que los identificadores y conectores de datos logran llegar a la identidad podría dar cobertura legal a una gran variedad de tratamientos de categorías de datos (no solo políticos). Prácticas que podrían ser tan criticables como lo son las que se realizan en países¹⁷ sin el reconocimiento de este derecho fundamental¹⁸, y sin una legislación general estricta y garantista del derecho como lo es la europea.

La habilitación legal del «interés público» para el tratamiento de estos datos especiales (art. 6.1.e. Reglamento) se presenta a lo largo del articulado justificando excepciones, exenciones y limitaciones al derecho fundamental de protección de datos personales. Se establece una disposición general para que los Estados puedan utilizarla:

¹⁴ «Constitutional attention to informational privacy must move beyond simply protecting personal data associated with deliberative democracy; rather, it should also offer safeguards when an individual's underlying capacity for decisionmaking is threatened» (Schwartz, 1995: 557).

¹⁵ Afirmar 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».

¹⁶ Paul Ohm se enfoca en «highlighting the difficulty of protecting the privacy of data subjects by anonymizing data»; Paul M. Schwartz y Daniel J. Solove, en «discussing identification of individuals from personally identifiable information found from data sources», y Rebecca J. Rosen, en «explaining the ease with which metadata can be matched with specific individuals».

¹⁷ Concretamente, Estados Unidos: casos *Cambridge Analytica* o el del analista de la CIA Snowden.

¹⁸ Carta de los Derechos Fundamentales de la Unión Europea (2016/C202/02): arts. 7 y 8.

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 [...]. 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.

Queda, básicamente, en manos de los Estados aquilatar lo que debe ser «ese interés público» para el tratamiento de estos datos especiales y en lo que se entienda que requiere el «funcionamiento democrático» en cada momento. Quien decida que lo exige el funcionamiento democrático debería especificarlo dicha norma (las redes de colaboración de autoridades de la recomendación de la Comisión es un ejemplo). Un estudio reciente de derecho comparado (Rubinstein *et al.*, 2014: 97) ha analizado cómo utilizan 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 (*ibid.*: 103).

2.1. La prohibición general del tratamiento de datos sensibles de opinión política: su excepción por interés público

El art. 9.1. del Reglamento establece la prohibición general de tratamiento de datos sensibles o especiales, entre ellos, las opiniones políticas. Pero el art. 9.2. establece que el art. 9.1. no será de aplicación cuando «el tratamiento es necesario por razones de interés público esencial [...]» (9.2.g). Sin embargo, ya el considerando 52 adelantaba: «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 en el mismo art. 9.2., apartado d), establece, además, que la prohibición general no se aplica, extendiendo más el círculo de excepciones, cuando el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una asociación¹⁹ cuya finalidad sea política (en este caso) y el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de

¹⁹ Los partidos políticos no son poderes u órganos del Estado; conforme a la STC 3/1981, son asociaciones políticas que llevan a cabo funciones públicas. Como tal,

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». Se asume que los miembros de un partido, en cuanto que asociación, por el hecho de la filiación, consienten en todo momento el tratamiento de sus datos con finalidad política y en el ámbito de la organización. Esta disposición, ya prevista en la legislación anterior, no es el objeto específico de este trabajo, aunque, obviamente, también se puedan valer de ella los partidos para sus actividades legítimas. La previsión del considerando 56 tiene para los partidos una finalidad más ambiciosa: dirigida a las «actividades electorales» «para el funcionamiento democrático» (excede a la propia organización), por razones de interés público (que justifican numerosas limitaciones), y puede afectar a los datos de «todas las personas», no solo de sus miembros o simpatizantes. Aun así, este art. 9.2 provoca inquietud respecto a la calidad de los datos de los antiguos miembros, o a la extensión del número de personas a las que se puede alcanzar si se piensa en el contexto electrónico de los posibles «contactos regulares» (minimización de los datos).

Una cuestión previa, de gran calado, es qué se entiende por datos personales sobre las «opiniones políticas de las personas». «Opinión política» es, en sí, un concepto indeterminado, cuya imprecisión se agrava en este contexto digital, y máxime si se une a los datos personales de «las personas» (de todas). Por un lado, se entiende que las opiniones políticas son el resultado del ejercicio del derecho a la libertad de expresión, pero por otro se puede asociar con la «opinión pública» misma, concepto igualmente indeterminado. El legislador ha puesto intencionadamente el foco de atención en los datos personales de las opiniones políticas para el funcionamiento democrático. Los datos de opinión al servicio de los partidos deben responder, por tanto, a alguna necesidad general.

Siendo un eje clave, resulta imprescindible acotar bien «opinión política» y su espectro objeto de tratamiento. También lo que es «actividad electoral», a efectos de aplicar el Reglamento: si debemos atenernos a la LOREG, y entenderla como «acto de campaña electoral» estrictamente (art. 53 ley electoral); o si se podría calificar de «actividad electoral», en sentido más general, a lo que se ha denominado «campaña permanente» (Ornstein y Mann, 2000: 162). Y si la recopilación de datos de opinión podría ser calificada como «acto de campaña», «publicidad política» o «propaganda electoral», utilizando los términos de la ley. 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

pueden atraer 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).

continuada, latente y no explícita (Jason, 2015: 46)²⁰. 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 (datos) de los ciudadanos en la Red (Kosinski *et al.*, 2013), difundiendo información *ad hoc* según sus perfiles y, quizá ya en campaña electoral, exponiendo a los distintos segmentos de población identificados a mensajes claramente propagandísticos. Se diría que la propaganda se ha liberado del «corsé legal» de la campaña electoral, y puede manifestarse de otras maneras más efectivas. Parafraseando a Stanley Jason, «la propaganda peligrosa en una sociedad democrática es aquella que no es reconocida como propaganda» (Jason, 2015: 46).

Sin perjuicio de que pueda definir técnicamente qué es un mensaje de opinión (García Sanz, 1990), la realidad digital muestra que hay muchas maneras²¹, elementos, comportamientos y 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. No creo que el legislador ignore la capacidad de la técnica de «vulnerar continuamente» la privacidad de las personas, como bien señala el considerando 30 del Reglamento.

Pero el Reglamento ofrece, inaplicando la prohibición general, 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) [...] 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 al tratamiento de distintas categorías de datos: utilizando las herramientas que recoge el considerando 62, y otras muchas disponibles, para recabar e identificar a las personas y sus opiniones. Siendo tantas las fuentes y posibilidades de obtener opiniones políticas (y no políticas) y asociarlas a personas físicas, el legislador debió tener en mente la pseudoanonimización, como medida técnica de seguridad y gestión de las posibles bases de

²⁰ El autor diferencia entre la «classical conception of propaganda» y «propaganda as biased speech». Y diferencia la propaganda que se realiza en los países totalitarios de la que llevan a cabo las democracias liberales: «It 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 nonpropagandistic claims are in fact propaganda», p. 46. Esta confusión se acrecienta en la Red.

²¹ Los *likes* en Facebook, nuestras búsquedas en Google, los datos que revelan nuestro navegador, los *retuits*, etc.

datos ideológicas. Pero solo la técnica es insuficiente, se necesita la colaboración de la ley. La excepción de interés público podría cubrir una gran variedad de acciones (incluso decisiones automatizadas o perfiles)²². Y las medidas de seguridad deben extremarse cuantas más personas estén expuestas, pues la vulneración de los datos sensibles puede causar daños²³ impredecibles. En este sentido, hay que atender al Reglamento, que en el considerando 71 advierte de los riesgos, especialmente, de las posibles discriminaciones por opiniones políticas. Además, afirma: «Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas».

Parece 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 que el consentimiento, y la posibilidad de informar solo *a posteriori* puede ser ineficaz. Y a efectos de actividades electorales, permiten «observar y certificar» estados de opinión (que bien pueden haber sido manipulados y creados en Internet).

2.2. La habilitación legal del interés público para tratar los datos sensibles de las opiniones políticas por los partidos políticos en el marco de actividades electorales

En principio, cabe preguntarse a qué partidos políticos y a qué miembros del mismo se está refiriendo el Reglamento: si a los que la ley electoral vigente reconoce (representantes) o si es necesario ser más granulares en el contexto del Reglamento (afiliados, simpatizantes, votantes). Ya advertía Rubio (2011: 319-321) de los problemas que planteaban las nuevas tecnologías para reconocer a los sujetos implicados en la campaña, y de la necesidad de distinguir según los medios (convencionales o no). Hay que llamar la atención sobre que las medidas de la Unión Europea recientes no contemplan la acción del votante o ciudadano en la campaña.

Y no es un matiz baladí. Pues, ciñéndonos solo a tratamiento de datos, quién esté legitimado cuenta con numerosos artículos de gran trascendencia: así, el art. 23.1. sienta el principio general para establecer los límites al derecho fundamental (y el 23.2, las disposiciones específicas mínimas relativas a la medida anterior).

²² En los puntos 9 y 22 de la resolución del Parlamento, citada, se «insiste en que la publicidad política y electoral no debe realizarse sobre la base de perfiles de usuarios individuales».

²³ Véase el considerando 85 del Reglamento de Datos.

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.

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 han sentado²⁴ para que la norma que regule la vigilancia y el acceso a datos, a extramuros de la ley general, sea conforme a los derechos fundamentales.

Debería pensarse 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. Y ello tanto en el proceso electoral como después en sede parlamentaria, fortaleciendo los principios del trabajo parlamentario, sin sustituirlo (Aranda, 2017: 43). El principio de legitimidad democrática, el pluralismo político y los partidos políticos (art. 6 CE) pueden quedar falseados de contenido y pervertida su función si la vigilancia, recopilación y uso de los datos en relación a las opiniones políticas de los ciudadanos, invadiendo intensamente la privacidad, pudieran ser el medio para «manipular» la voluntad de voto socavando su libertad²⁵. Quiere decirse, una «restricción» intensa del derecho a la protección de datos no redundaría en la expansión y preferencia del derecho de participación, sino todo lo contrario. Afectando tanto al derecho de sufragio como al derecho de participación que ejercen los partidos, en cuanto que grupos parlamentarios en el Parlamento (Rubio, 2014; Aranda, 2017). Situación que ahondaría más en la desconfianza entre representantes y representados lamentablemente, si no se establecen controles oportunos.

Sin perjuicio del citado art. 23 del Reglamento, disponen de una amplia batería de disposiciones, pues siempre van a necesitar una base legal para tratar estos datos (art. 6.2 del Reglamento). Entre otras, en los apartados 6.1.c), 6.1.e) y 6.1.f) tienen más fundamentos para el tratamiento de los datos respecto a las

²⁴ Sentencia del Tribunal de Derechos Humanos de Estrasburgo, de 29 de junio de 2006. *Weber and Saravia v. Germany*, 54934/00, §§78-79. Establece criterios para realizar el test de la norma.

²⁵ En esta dirección van las disposiciones de la citada propuesta de reglamento en lo que respecta a infracciones de normas de protección de los datos personales.

opiniones de las personas (y si es el Gobierno, podría recurrir a más razones convincentes e incluso a otros fundamentos, fuera de la ley electoral). Así se lee:

6.1.c) [...] el tratamiento es necesario para el cumplimiento de una obligación legal; [...] 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, [...].

Pero si no satisfacen las anteriores, a falta de norma habilitante, el art. 6.4 pone a disposición otro recurso, escapando a las previsiones anteriores: cuando el tratamiento sin el consentimiento «constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23.1».

Aún más, el art. 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): «[...] recogidos con fines determinados, [...]»; 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 generar bases de datos ideológicas y la posible creación de psicoperfiles, amén de otras utilidades que puede propiciar el *big data analytics*, en período electoral o en campaña permanente. El principio de «limitación de conservación» debería estar presente.

El legislador debería ser escrupuloso al regular el uso de datos de las opiniones por los partidos (para no ahondar más la crisis de confianza con la ciudadanía), si lo que se pretende es conectarlos con las personas y «reformular» su función de conformadores de la opinión pública. Concepto de opinión pública que, más que nunca, se encuentra en crisis (Torres del Moral, 2013: 1393), a consecuencia de Internet y sus prácticas comunicativas. La concreción con que se determinen, entre otros, los extremos aquí planteados tiene consecuencias distintas para el funcionamiento democrático. Y ello tanto en el procedimiento y las reglas para la elección de representantes y gobernantes como en la manera de organización política (preámbulo de la CE, art. 1). La campaña electoral se ha desplazado a Internet. El legislador debe concretar sus principios en los medios electrónicos²⁶, con tanta o mayor minuciosidad a la practicada para los medios de comunicación convencionales.

²⁶ En este mismo sentido, el punto 23 de la resolución del Parlamento citada.

Son muchas las oportunidades pero también muchos son los riesgos. El *big data analytics* y algunas herramientas diseñadas para el análisis político electoral pueden identificar a cada votante y su perfil opinático. Permiten fraccionar la sociedad y comunicar mensajes a medida de cada votante individual con el fin electoral que se persiga. Las nuevas tecnologías de la información, *software*, algoritmos (Reitinger, 2015)²⁷ y/o la inteligencia artificial y el *big data analytics* lo posibilitan si no se dan los controles y garantías necesarios. El pluralismo político-ideológico que caracteriza la democracia contemporánea —propiciado en gran parte por los medios convencionales— podría desvanecerse; así como el imperio de la ley como expresión de la voluntad general —pues la voluntad del pueblo puede no ser ya la del pueblo— (Rubio y Vela, 2017a: 109-113)²⁸. Pero no todo son malas noticias, también hay aspectos muy positivos. Los grupos parlamentarios podrían utilizar estas habilitaciones de «interés público» (en las condiciones de excepcionalidad señaladas) para que la legítima comunicación parlamentaria, que tiene una función política de «institucionalización de lo que ya es público», se transmita con acierto y, a la vez, sirva para que «el Parlamento cobre un mayor protagonismo en la producción de la política» (*ibid.*: 112). Además, el uso de las TIC que hacen los grupos parlamentarios, en lo que se va llamando «parlamento abierto» (Rubio y Vela, 2017b), podría verse revitalizado si se corrigen esos riesgos en la formación de la opinión pública, siempre que se utilice la habilitación del Reglamento con los controles previstos. Se ha detectado un problema añadido a un uso indebido o excesivo de los datos que comunican los ciudadanos, por los canales de comunicación directa con los Parlamentos²⁹ a través de sus plataformas: quedan reflejados sus opiniones y datos en muy diversas cuestiones³⁰, y pueden producirse tratamientos sin control. Cabe sugerir que se podrían diseñar estas plataformas para que la comunicación pudiera ser anónima (Martin y Fargo, 2015)³¹, en la medida de lo posible técnicamente, si el ciudadano así lo desea. Sería una ironía que la pretendida transparencia y el aclamado

²⁷ Véase también la conferencia de la NYU: «Governing Algorithms. A Conference on Computation, Automation, and Control», New York University, 16 de mayo de 2013.

²⁸ «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: [...]», p. 109.

²⁹ La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

³⁰ Problema que ya ha sido advertido en Italia: el *Provvedimento* de 6 de marzo de 2014 prevé expresamente que no pueden ser utilizados para fines de campaña electoral los datos personales disponibles en estas plataformas públicas.

³¹ Los autores defienden la necesidad de un «derecho de anónimo» de la persona.

derecho de acceso se convirtieran en una «trampa a la democracia» debido a un uso de los datos que traspase los límites legales en aras del «interés público», al servicio de la democracia.

III. «INTERÉS PÚBLICO»: UN CONCEPTO JURÍDICO INDETERMINADO PARA LIMITAR (Y POSIBLEMENTE DESNATURALIZAR) EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

El derecho a la protección de datos personales es un derecho fundamental y un derecho instrumental (Canals Ametller, 2016: 14) que sirve especialmente para proteger la privacidad de las personas, pero no solamente, porque su carácter irradiante se extiende a los demás derechos fundamentales. El interés público es base jurídica del tratamiento (art. 6.1.c) y límite a numerosas facultades y obligaciones que configuran el derecho fundamental (art. 23.1). Límites formulados con tanta amplitud que permitirían fácilmente la intromisión en el contenido esencial y desnaturalizar el derecho (González Fuster, 2015: 532)³². La extensión de estos límites tendría consecuencias en otros derechos, especialmente en el de privacidad y en el de participación política. Resulta necesario medir las posibles limitaciones previstas en el Reglamento (arts. 6.2 y 6.3.b), y los elementos sobre los que recaen deben ser identificados granularmente (art. 23.2): límites subjetivos (sujetos), límites objetivos (o materiales), límites en el contenido, límites temporales y espaciales. Determinando tanto la finalidad como la base jurídica que legitima el tratamiento. Límites que deberían interpretarse muy restrictivamente.

1. MIDIENDO LOS LÍMITES AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

1.1. Base jurídica

La base jurídica, que el Reglamento refiere en general al «interés público», hay que especificarla para una regulación precisa (la identificación y/o formación de la voluntad popular electoral). En el Reglamento, la base jurídica del «interés

³² La autora ha analizado la falta de certeza respecto al contenido esencial del derecho y la heterogeneidad de límites de distinto alcance que permite el Reglamento. «The limited case law of the EU of Court of Justice on the right's essence does not help to provide clear answers to this discussion».

público» no está constituida como excepción al principio general del «consentimiento» para el tratamiento de datos personales, como ocurría en la legislación anterior —véase el art. 6.1.e)—. Actúa a su mismo nivel y con la misma legitimidad, en multiplicidad de situaciones y realidades. Lo que permite una gran capacidad de maniobra a los partidos, así como la utilización de múltiples límites a los principios, obligaciones y derechos esenciales que reconoce la ley a la persona titular del derecho: por ejemplo, el derecho de información del afectado por el tratamiento o el de oposición cuando no se basa en el consentimiento (arts. 12, 13 y 21)³³; pueden también quedar excepcionadas las prohibiciones de realizar perfiles ideológicos, y/o de decisiones automatizadas sobre las personas (inteligencia artificial, art. 22). No obstante, conviene recordar que la habilitación legal del interés público solo lo es con fin electoral. Para otros fines debería mediar el consentimiento del afectado (STC 292/2000, de 30 de noviembre), siempre que sea posible técnicamente, u otra base jurídica posible de las citadas.

1.2. Finalidad

La finalidad hay que especificarla para una regulación precisa: la formación de la voluntad general para el «funcionamiento democrático». El art. 5.1.b) del Reglamento exige, además, que sean fines determinados, explícitos y legítimos. Ello obliga a concretarlo más y a dirigirlo al «marco de actividades electorales». En virtud del «principio de limitación de la finalidad» —art. 1.e.)—, este fin electoral debe ser debidamente concretado: si son actividades electorales que se someten o no al derecho de la Unión (y consiguientemente si se aplica directa o supletoriamente el Reglamento), si son actividades electorales en lo que se ha llamado «campana permanente», o en precampaña o propiamente durante la campaña electoral. Esta acotación no es menor, pues el volumen de datos que se pueden recopilar y tratar nos pone de lleno en la problemática jurídica del *big data* y de las macrobases de datos ideológicas (García Mahamut, 2015: 332). El uso masivo y personalizado de datos tratados por los algoritmos e inteligencia artificial permite multiplicidad de operaciones, como sofisticados perfiles ideológicos, la toma de decisiones automatizadas, la realización de programas electorales, o el diseño de políticas sobre patrones precisos de la minería de datos. Lo que podría tener alguna justificación, si cabe, en campaña electoral —como una situación excepcional en materia de datos e información—, a semejanza de lo que se establece en la actualidad respecto al régimen vigente de los medios de comunicación en campaña electoral (Holgado González, 2017: 465). Pero dejaría de tener un fundamento

³³ Arts. 156 y ss. Reglamento de Datos: transparencia proactiva y posterior.

legítimo si se hace «permanentemente», o frecuentemente, aún en el marco de actividades electorales (Rubio, 2011: 329-331). Salvo por razones de amenaza democrática, tal monitorización permanente produciría un *chilling effect* sobre otros derechos fundamentales, como el de la libertad ideológica o el de la libertad de expresión e información, vitales para el pluralismo político. Y, por supuesto, podría dejar vacío de contenido al derecho de sufragio.

1.3. Sujetos

El Reglamento refiere en general a personas y partidos. Puede ser conveniente diferenciar las diferentes categorías subjetivas para marcar líneas precisas de regulación. Diferenciando sujeto pasivo (todas las personas) y sujeto activo (los partidos). Y dentro de la primera, habría que distinguir si solo los datos de los electores o si podría extenderse a otros. En la legislación del censo está resuelto claramente, pero no en el Reglamento. La referencia a «todas las personas» se expande a cualquier persona que participe en la Red. Y podrían sus datos personales ser objeto de tratamiento con fines políticos. Teniendo en cuenta el carácter global de la red —y en concreto las redes sociales—, cualquier persona de cualquier lugar puede ser observada y recopilados sus datos con estos fines³⁴. En cuanto a la segunda categoría, se debería especificar si solo los representantes de las candidaturas y representantes generales, o si se autoriza a otros miembros y cuáles. Asimismo, la extensión de la autorización, para evitar ventajas competitivas en la contienda electoral (García Mahamut, 2015: 324).

1.4. Objeto

El Reglamento refiere en general a los datos personales de las opiniones políticas. Es necesario nombrar granularmente las diferentes categorías de datos que se pueden incluir, para marcar líneas de regulación precisas en cuanto al ámbito material de la norma. El espectro de datos podría ser ilimitado, por la capacidad de las herramientas tecnológicas para deducir o inducir ideología de los diferentes movimientos u opciones que se hacen en Internet. Precisar qué pueden hacer o no pueden hacer con estos datos los partidos, o, lo que es lo mismo, qué tratamientos son permitidos y prohibidos (deben ceñirse al fin). Una limitación taxativa respecto a las herramientas que se permiten para la recopilación y el tratamiento. Además, si las bases de datos ideológicas se permitiesen (art. 9.2.j), su diseño técnico podría resolver muchas

³⁴ Como bien ha recogido la resolución del Parlamento en su punto 9.

cuestiones, en todo su ámbito de aplicación, incluidos fines, tiempo, espacio y medidas de seguridad (el Reglamento contempla el *privacy by design*, art. 25). Y si se califican estas con fines de archivo, investigación o estadística en interés público, podría no haber restricción temporal (arts. 89.1. y 5.1.e).

De nuevo, hay que llamar la atención acerca de que se está ante datos sensibles, que reciben un especial tratamiento —art. 9.1. del Reglamento—, y que por razones de interés público se excepcionan de tal tratamiento —art. 9.2.g)—. Qué son «opiniones políticas» puede tener una muy difícil concreción en el mundo virtual de Internet. La indeterminación de lo que pueda ser opinión política en la Red conlleva a la indeterminación de los datos personales que pueden recopilarse o tratarse. En definitiva, no se cumpliría con el principio de minimización de los datos, que deben ser, además, adecuados, pertinentes y limitados al fin —art. 1 c) Reglamento—. Y el hecho de que se recopilen «en el marco de actividades electorales» es una referencia muy amplia que no aclara nada.

1.5. Tiempo

El Reglamento solo dice «en el marco de actividades electorales». Sería útil distinguir diferentes categorías temporales para marcar líneas precisas de regulación. Diferenciar, siguiendo a la LOREG, si actividades en el tiempo limitado de la precampaña o campaña propiamente, o si en cualquier tiempo siempre que la actividad tenga una finalidad electoral (campaña permanente). La categorización de los tiempos podría conducir a una modulación de los límites y las garantías, siendo estos más intensos en la campaña propiamente, y en armonía con los principios jurídicos que deben presidir la contienda electoral.

1.6. Espacio

El Reglamento refiere en general a los «Estados miembros», la «Unión» y al sistema democrático. Habría que precisar categorías espaciales posibles en Internet para una regulación efectiva. Sin olvidar que la red es global y presenta dificultades para identificar la ubicación, o distinguir el espacio público del privado (Rubio, 2011: 326-327). Difícil, pero no siempre imposible marcar la trazabilidad: por la dirección IP de conexión o la ubicación de los servidores (sirvan de ejemplo). Técnicamente³⁵ es posible revelar el origen de los

³⁵ El punto 8 de la resolución Europea citada: «Considera que el requisito de verificar la identidad, la ubicación y el patrocinador de la publicidad política recientemente introducida por Facebook en los Estados Unidos es una buena iniciativa que aumentará

datos, detectar injerencias y desenmascarar la posible falsa «voluntad popular» en un Estado miembro. Además, interpretando el espacio virtual como el de la democracia digital y admitiendo como fuentes los distintos espacios de comunicación electrónica (redes sociales, blogs, webs, metadatos, etc.), se podría delimitar qué fuentes son accesibles para los partidos y restringir de esta manera las categorías de datos dentro de lo posible (minimización y calidad de los datos).

1.7. Contenido

El Reglamento establece, en general, límites por razón del interés público a las distintas facultades y obligaciones que contiene el derecho. Una diferenciación granular de diferentes categorías de límites ayudaría a marcar líneas de regulación precisas. En principio, cabe distinguir entre límites que imponga la norma y límites mismos que impone la tecnología por su propia naturaleza y funcionamiento. El art. 23.1, reproducido más arriba, establece en general el elenco de límites, pero después existen otros que vienen dados específicamente por el interés público, se ha visto en el epígrafe anterior. Son muchos los límites y deben ser restringidos en el tiempo, espacio, sujetos, objeto y finalidad, a riesgo de vaciar de contenido el derecho fundamental. Y someterse a las máximas garantías legales y medidas técnicas de seguridad que ofrece el mismo Reglamento.

2. APARENTE CONFLICTO DE DERECHOS FUNDAMENTALES: UNA PERSPECTIVA DESDE SU DIMENSIÓN INSTITUCIONAL

Al hilo de lo previamente expuesto, podría afirmarse que existe una tensión entre el derecho a la protección de datos personales y el derecho de participación. Sin embargo, como se va deduciendo, tal conflicto en realidad no existe. Y no existe porque si no se respeta el contenido esencial de uno, se desnaturaliza también el del otro. Una regulación invasiva del derecho a la protección de datos invadiría la privacidad de las personas; dejaría vacío de contenido no solo al derecho a la protección de datos personales, sino también al derecho a la privacidad, y sin sentido a los derechos de participación, especialmente al derecho de sufragio, «nervio y sustento de la democracia» (STC 24/1990, FJ 2). Y no podría garantizarse la «delegación de la soberanía en los representantes del pueblo, que constituye la primera parte y la más

la transparencia y contribuirá a la lucha contra la intromisión electoral por parte de agentes extranjeros» (trazabilidad).

importante de la cadena de legitimación ininterrumpida del pueblo a los órganos y cargos públicos» (Fernández Riveira, 2011: 185). Se podría afirmar que la habilitación legal y las limitaciones previstas por el Reglamento deben interpretarse muy restrictivamente: optar por categorías en su mínima expresión invasiva, que favorezcan el conocimiento de la voluntad popular y ayuden en la formación de la opinión pública, dando un trato preferencial al derecho de participación, con fin electoral, en la medida que lo requiera el funcionamiento democrático. Entendiendo que ese «si lo exigiera el funcionamiento democrático» significa situaciones taxadas y en momentos puntuales. Ahora bien, la ponderación es delicada. Se requieren medidas legales, técnicas y organizativas que garanticen la legalidad de estos tratamientos excepcionales (Rubinstein *et al.*, 2014: 114).

Una perspectiva institucional de la campaña electoral y de los derechos implicados puede aportar una visión armónica para realizar los cambios necesarios con fin democrático. El acomodo de estos derechos tiene un engranaje adecuado desde esta perspectiva. La campaña «clave de la bóveda del régimen democrático», en palabras de García Mahamut (2015: 321), y sus principios —libre concurrencia, competitividad e igualdad de oportunidades— han perdido eficacia, y se requiere su «nueva versión» en los medios electrónicos. En este contexto, la recopilación de los datos personales y su utilización para la difusión de mensajes electorales es clave. Señala De la Quadra (2017: 16), referido a la dimensión institucional, que «la delimitación de los derechos no queda petrificada en un momento de la historia, sino que se va adecuando al espíritu de la época». El legislador puede delimitar (que no limitar) el contenido esencial atendiendo a su función social, sin dejarlo irreconocible, pues sería inconstitucional (art. 53 CE). Pero si traspasa el ámbito de la delimitación incurriría en lo que a veces se llama expropiación legislativa, por privación de derechos singulares, o en responsabilidad por las restricciones que impone (*ibid.*: 17). En la misma línea, y siguiendo la idea de proceso electoral desde un perspectiva institucional, entiende Solozabal (1993: 64) que el «enfoque institucional del Derecho electoral propone en primer lugar una interpretación de éste adecuada a su finalidad —la obtención de una representación política en correspondencia tan próxima como sea posible a la voluntad del cuerpo electoral—. Esta posición justificaría la habilitación a los partidos para recopilar y tratar datos, con el fin de identificar y formar la voluntad popular; y justificaría las delimitaciones necesarias al derecho a la protección de datos en esas situaciones de excepcionalidad, con el fin de que el ejercicio de los derechos de participación despliegue toda su eficacia en el proceso electoral. Ahora bien, sin incurrir en restricciones que supongan la desnaturalización del derecho y la invasión en la privacidad de la persona. Evitando el posible *chilling effect* en otros derechos.

Los principios electorales, y el papel de los datos personales en los mismos, hay que repensarlos en el soporte electrónico³⁶: cuanta más intromisión sin la legitimación del consentimiento (usando otras bases jurídicas), menos posibilidades de un proceso electoral y democrático conforme a derechos los constitucionales.

En España las normas electorales, aunque hayan integrado nominalmente a los medios electrónicos³⁷, resultan insuficientes. La regulación del censo electoral³⁸, en razón a su fin, está fuera del ámbito de aplicación de la legislación de protección de datos. Aunque cumplido su fin, declaró el TC, no se debían tratar sus datos personales sin el consentimiento de la persona (STC 292/2000, de 30 de noviembre). El nuevo art. 58 bis³⁹ (por «interés público» pueden aplicar numerosas excepciones), en su apartado primero, párrafo primero, señala que podrán recabar datos personales de las opiniones políticas «en sus actividades electorales»; mientras que en el párrafo segundo añade que pueden recabar «datos personales» en «actividades políticas» en «periodo electoral», en ambos sin mayor especificación. Todo ello provoca incertidumbre, que se une a la que producen los términos «webs y otras fuentes de acceso público», sin diferenciar si refiere a las mismas conforme a la legislación de datos o en cuanto a su acceso no restringido al público⁴⁰. La única garantía expresa aquí es el derecho de oposición, en el modificado del art. 39.3. LOREG (para la propaganda electoral vía postal), y en el mismo art. 58 bis 5, para la propaganda vía redes sociales, mensajería y todo tipo de medios electrónicos.

Los titulares del derecho de participación son los ciudadanos, los partidos son solo su instrumento, según doctrina del Tribunal Constitucional (STC 64/2002). Y deben preservar la privacidad de las personas para que la participación sea real, y si se requieren datos personales de las opiniones

³⁶ Los puntos 4 y 5 de la resolución del Parlamento citada barajan una variedad de principios para las campañas en línea: transparencia y responsabilidad algorítmica, etc. Llama la atención que la resolución se enfoque en medidas limitativas y prohibitivas a imponer a las plataformas de las tecnológicas, pero que no preste atención al mismo tiempo a las amplias legitimaciones de tratamiento que contiene el Reglamento para los partidos.

³⁷ Instrucción 4/2007, de 12 de abril, e Instrucción 3/2011, de 24 de marzo, ambas de la Junta Electoral Central. Y ahora también el nuevo art. 58 bis LOREG.

³⁸ LOREG, modificada el 2-11-2016. Art. 41: Real Decreto 1799/2003, de 26 de diciembre, por el que se regula el contenido de las listas electorales y de las copias del censo electoral modificado, por el Real Decreto 288/2014, de 25 de abril.

³⁹ LOREG.

⁴⁰ Ejemplo, el censo electoral.

políticas con el fin de satisfacer el derecho de sufragio, la transparencia debe ser garantía previa que acompañe a todas las demás⁴¹. Si se aniquila la privacidad de las personas (incluida la de los partidos), se aniquilan la misma libertad como derecho, y el mismo presupuesto del ejercicio de los otros derechos (Rallo Lombarte, 2017: 595). Recuerdan Schwartz y Peifer (2017: 119): «The EU has created a privacy culture around “rights talk”⁴² that serves to protect “data subjects”. In the EU, rights talk forms a critical part of the postwar European project of creating the identity of a European citizen. As Jürgen Habermas argues, this task is a constitutional one that is central to the EU’s survival». Lo contrario significaría un suicidio institucional por parte de los propios partidos, que requieren, como asociaciones, también, de los derechos de privacidad, entre otros, para asegurar su pervivencia.

IV. CONCLUSIONES

a) El Reglamento abre las puertas legalmente a una amplitud de posibilidades de recopilación y tratamiento de datos personales de las opiniones políticas, con fines electorales, por parte de los partidos políticos por razones de interés público. Igualmente, disponen de una batería de límites al derecho fundamental justificados por el interés público. Estos recursos legales, unidos a las sofisticadas herramientas tecnológicas, permitirían traspasar el contenido esencial del derecho y dejar sin efecto otros derechos fundamentales.

b) La habilitación del legislador a los partidos políticos, con fines electorales, se justifica por un interés público concreto que requiere el funcionamiento del sistema democrático: cuando se den circunstancias en los medios electrónicos que falseen la opinión pública y el pluralismo político, y, por tanto, impidan el buen funcionamiento democrático, puedan, entonces, los partidos acceder a los datos personales de las opiniones políticas, identificar la auténtica voluntad popular y cumplir con su función constitucional para que los procesos democráticos se den conforme a derecho.

c) El conflicto entre los derechos fundamentales de protección de datos personales y el derecho de participación (concretamente el derecho de sufragio) es solo aparente. Si no se delimita muy bien el primero, y se interpretan muy restrictivamente sus límites, se podría producir una desnaturalización del derecho fundamental de protección de datos, que conllevaría a una invasión de la privacidad de las personas. Tal acción invasiva en el derecho fundamental

⁴¹ Ley de Transparencia y art. 12 del Reglamento.

⁴² Significa, en este contexto, derecho a la protección de datos personales.

de privacidad podría pervertir el propio derecho de sufragio, que, ejercido sin libertad, falsearía los resultados electorales y al mismo sistema representativo.

d) Se deben determinar y acotar cada uno de los términos de los límites para que puedan cumplir una finalidad institucional: depurar y formar la opinión pública electoral, para que el derecho de participación despliegue sus efectos en los procesos democráticos y en la campaña electoral, que se sustancia «en línea» como una realidad de hecho. Sus principios jurídicos deben de repensarse en digital, siguiendo la resolución del Parlamento Europeo citada.

Bibliografía

- 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. Disponible en: <https://doi.org/10.18042/cepc/redc.111.01>.
- Bastida Freijedo, F. J. (1994). *El régimen jurídico de la comunicación social*. Madrid: Instituto de Estudios Económicos.
- Bustos Gisbert, R. (2017). *Calidad democrática. Reflexiones constitucionales desde la teoría, la realidad y el deseo*. Madrid: Marcial Pons.
- Canals Ametller, D. (2016). El acceso público a datos en un contexto de transparencia y de buena regulación. En D. Canals Ametller (ed.). *Datos. Protección, transparencia y buena regulación* (pp. 11-52). Girona: Documenta Universitaria.
- Cukier, Kenneth C. y Mayer-Schoenberger, V. (2013). *Big Data: A Revolution That will Transform How We Live, Work and Think*. New York: Houghton Mifflin Harcourt.
- Fernández Miranda, C. y Fernández Miranda, A. (2003). *Sistema electoral, partidos políticos y Parlamento*. Madrid: Editorial Colex.
- Fernández Riveira, R. (2011). Es inconstitucional el voto electrónico en Alemania? En J. Barrat i Esteve y R. Fernández Riveira (coords.). *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías* (pp. 157-194). Pamplona: Thomson Reuters.
- García Mahamut, R. (2015). Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflicto en el ordenamiento español. *Teoría y Realidad Constitucional*, 35, 309-338. Disponible en: <https://doi.org/10.5944/trc.35.2015.14921>.
- García Sanz, R. M. (1990). *El derecho a opinar libremente*. Madrid: Editorial Eudema.
- (2017). *Digital Journalism. Rethinking Communication Law to Support Democracy and Viable Business Models*. Palo Alto: Academica Press.
- González Fuster, G. (2015). Curtaling a right in flux: restrictions of the right to personal data protection. En A. Rallo Lombarte y R. García Mahamut (eds.). *Hacia un nuevo Derecho europeo de protección de datos* (pp. 513-537). Valencia: Tirant lo Blanch.
- Holgado González, M. (2017). Publicidad e información sobre elecciones en los medios de comunicación durante la campaña electoral. *Teoría y Realidad Constitucional*, 40, 457-485.
- Jason, S. (2015). *How Propaganda Works*. New Jersey: Princeton University.
- Kosinski, M., Stillwell, D. y Graepel, T. M. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110 (15), 5802-5805. Disponible en: <https://doi.org/10.1073/pnas.1218772110>.

- López Calera, N. (2010). El interés público: entre la ideología y el derecho. *Anales de la Cátedra Francisco Suárez*, 44, 123-148.
- Martin, J. A. y Fargo, A. L. (2015). Anonymity as a Legal Right: Where and Why It Matters. *North Carolina Journal of Law and Technology*, 16, 311-375.
- Nissenbaum, H. y Barocas, S. (2014). Big Data's End Run around Anonymity and Consent. En J. Lane, V. Stodden, S. Bender y H. Nissenbaum (eds.). *Privacy, Big Data, and The Public Good: Frameworks for Engagement* (pp. 44-76). New York: Cambridge University Press.
- New York University 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>.
- Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701-1759.
- Ornstein, N. J. y Mann, T. E. (2000). *The Permanent Campaign and Its Future*. Washington DC: American Enterprise Institute; The Brookings Institution.
- Quadra-Salcedo, T. de la (2017). *Instituciones básicas del Derecho Administrativo*. Madrid: Universidad Carlos III.
- 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. Disponible en: <https://doi.org/10.5944/trc.39.2017.19150>.
- Reitinger, N. (2015). Algorithmic Choice and Superior Responsibility: Closing the Gap Between Liability and Lethal Autonomy by defining the Line Between Actors and Tools. *Gonzaga Law Review*, 51, 79-118.
- Rosen, R. J. (2013). Stanford Researchers: It Is Trivially Easy to Match Metadata to Real People. *The Atlantic*, 24-12-2013. Disponible en: <https://bit.ly/2DqJLap>.
- Rubinstein, I. S., Nojeim, G. T. y Lee, R. D. (2014). Systematic government access to personal data: a comparative analysis. *International Data Privacy Law*, 4 (2), 96-119. Disponible en: <https://doi.org/10.1093/idpl/ipu004>.
- Rubio Núñez, R. (2011). Nuevas tendencias de regulación del uso de las nuevas tecnologías en campaña electoral. En J. Barrat i Esteve y R. Fernández Riveira (coords.). *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías* (pp. 313-333). Pamplona: Thomson Reuters.
- (coord.). (2014). *Parlamentos abiertos. Tecnología y redes para la democracia*. Madrid: Congreso de los Diputados.
- Rubio Núñez, R. y Vela Navarro-Rubio, R. (2017a). *Parlamento abierto. El Parlamento en el siglo XXI*. Barcelona: Editorial UOC.
- (2017b). *El Parlamento abierto en el mundo, evolución y buenas prácticas*. Zaragoza: Fundación Manuel Giménez Abad.
- 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 Law Review*, 80, 557-618.
- Schwartz, P. y Solove, D. J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86, 1814-1894.

- Schwartz, P. M. y Peifer, K. N. (2017). Transatlantic Data Privacy Law. *The Georgetown Law Journal*, 106, 115.
- Solozabal Echavarría, J. J. (1993). Una visión institucional del proceso electoral. *Revista Española de Derecho Constitucional*, 39, 63-80.
- Torres del Moral, A. (2013). La opinión pública y su tratamiento jurisprudencial. *Constitución y desarrollo político* (pp. 1361-1396). Valencia: Tirant lo Blanch.
- Villaverde Menéndez, I. (1994). *Estado democrático e información: el derecho a ser Informado*. Oviedo: Junta del Principado de Asturias.
- 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 en: <http://dx.doi.org/10.5210/fm.v22i2.6936>.