Reflexiones sobre el marketing político y el fenómeno de la desinformación en el contexto electoral

Reflections on political marketing and the phenomenon of disinformation in the electoral context

Por ANA GARRIGA DOMÍNGUEZ
Universidad de Vigo

RESUMEN

La elaboración de perfiles en las plataformas sociales permite aplicar técnicas de micro-segmentación para elaborar información política personalizada. Se estudia la relación de estas técnicas con la difusión de noticias falsas y el fenómeno de la desinformación y su impacto en las libertades de expresión e ideológica y la institución de la opinión pública libre, que están en la base del sistema democrático, para después analizar el nuevo artículo 58 bis.1 de la LOREG.

Palabras clave: *vida privada, libertad de expresión, libertad ideológica, procesos electorales, microsegmentación, noticias falsas y desinformación en línea.*

ABSTRACT

Profiling on social platforms allows the application of microtargeting techniques to develop personalized policy information. The relationship of these techniques with the dissemination of fake news and the phenomenon of disinformation is studied as well as its impact on the freedom of expression

and ideology and the institution of free public opinion, underlying the democratic system. Finally, article 58 bis.1 of the General Electoral Regime Act is analysed.

Keywords: *privacy, freedom of expression, ideological freedom, electoral processes, microtargeting, fake news and disinformation online.*

I. INTRODUCCIÓN

El pasado mes de diciembre se aprobó la nueva ley de protección de datos personales y garantía de derechos digitales[1]. Su objeto, según se recoge en su exposición de motivos y en su artículo primero, es doble: por una parte, adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679, General de protección de datos[2] y completar sus disposiciones y, por otra, garantizar los derechos digitales de la ciudadanía según el mandato del artículo 18.4 de la Constitución. La Ley Orgánica 3/2018 ha nacido en medio de la polémica, lo que parece que es una tradición en nuestro país cuando se trata de

[1] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE de 5 de diciembre de 2018). En adelante LOPDyGDD.

[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) (DOUE de 4 de mayo de 2016). En adelante RGPD.

regular el derecho fundamental a la protección de datos personales. Sus predecesoras, la LORTAD[3] y La LOPD[4] fueron en su momento objeto de importantes críticas doctrinales[5] y de varios recursos de inconstitucionalidad[6].

Una de sus normas más controvertida es la disposición final tercera que modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG) para introducir el artículo 58 bis, que regula la utilización de medios tecnológicos y datos personales en las actividades electorales permitiendo, con las garantías adecuadas, la recopilación de datos personales relativos a las opiniones políticas de las personas por parte de los partidos políticos en el marco de sus actividades.

Se ha afirmado que esta norma permite el perfilado ideológico individual y, a pocos días de su aprobación, la presidencia de la Agencia Española de Protección de Datos (AEPD) hubo de emitir una nota informativa desmintiéndolo[7]. Posteriormente ha emitido un informe jurídico y aprobado una circular, que serán tratados más adelante.

Este trabajo pretende aportar una valoración de esta norma, pero también y ello debe hacerse previamente, una reflexión sobre la obtención de perfiles, particularmente ideológicos, y su relación con las libertades de expresión e información, las *fake news* y el fenómeno de la desinformación a través de la red y la institución de la opinión pública libre. Una de las ideas centrales de este trabajo es que existe una estrecha relación entre la garantía de la privacidad de las personas, especialmente a través del derecho fundamental a la protección de datos personales, y el ejercicio de las libertades de que nuestra constitución recoge en su artículo 20 y, en último término, con garantía de la formación de una opinión pública libre que está en la base del sistema democrático.

---

[3] Ley Orgánica 5/1992, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), BOE de 31 de octubre de 1992.

[4] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), BOE de 14 de diciembre de 1999.

[5] Por todos Pérez Luño, A. E., «Sobre el arte legislativo del birlibirloque. La LOPRODA y la tutela de la libertad informática en España», *Anuario de Filosofía del Derecho,* Tomo XVIII, 2001, y Sánchez Bravo, A. A., «La Ley Orgánica 15/1999, de protección de datos de carácter personal: diez consideraciones en torno a su contenido», *Revista de Estudios Políticos,* núm. 111, enero-marzo, 2001.

[6] Resueltos por el Tribunal Constitucional en sus sentencias 290/2000, de 30 noviembre (RTC 2000\290) y 292/ 2000 de 30 de noviembre (RTC 2000\292).

[7] El día 21 de noviembre de 2018 la AEPD emitió una Nota Informativa sobre el «Criterio de la Agencia Española de Protección de Datos sobre cuestiones electorales en el proyecto de nueva LOPD» afirmando que el texto del Proyecto de Ley no permitía el tratamiento de datos personales para la elaboración de perfiles basados en opiniones políticas, ni el envío de información personalizada basada en perfiles ideológicos o políticos (https://www.aepd.es/prensa/2018-11-21.html). Consultada el día 23 de noviembre de 2018.

II. EL CONTEXTO TECNOLÓGICO: *BIG DATA,* PERFILES Y ALGORITMOS PREDICTIVOS, PLATAFORMAS SOCIALES Y HUELLA DIGITAL

Nuestra vida se encuentra constantemente infiltrada por las tecnologías de información y la comunicación (TIC). Nosotros mismos facilitamos el seguimiento continuo de nuestra actividad a través del Smartphone, que nos acompaña a cualquier lugar al que vayamos y desde el que realizamos muchas acciones cotidianas además de comunicarnos con otros. No resulta exagerado referirnos a nuestro mundo como de sociedad del control[8] o sociedad de la transparencia[9] y se han normalizado las expresiones vigilancia masiva o vigilancia total. El 70% del universo digital es generado por nosotros mismos a través de nuestra interacción con los diferentes servicios de la red como los motores de búsqueda, las redes sociales, los *sitios* que visitamos en Internet, las compras que realizamos, los Smartphone, el correo electrónico, etc.[10]. Nuestra interacción en el mundo virtual, pero también en el físico es seguida y monitorizada por diversos vigilantes, que por diferentes razones e intereses, recogen y analizan nuestra actividad en los distintos servicios y redes de la Sociedad de la Información, pero también a través de diferentes dispositivos pertenecientes el mundo del Internet de las cosas[11], cada vez más populares, y que permiten registrar, por ejemplo, nuestros desplazamientos, número de pasos, pautas de sueño, pulsaciones, tensión arterial, temperatura, uso de electrodomésticos, etc.[12] En el mundo de la vigilancia líquida[13] cada uno de nuestros comentarios, acciones o intereses es susceptible de pasar a engrosar alguno de los muchos centros de datos que los Estados y las entidades privadas poseen y que en numerosas ocasiones constituyen su activo y objeto de negocio principal.

---

[8] Deleuze, G., «Postscript on the Societies of Control», october, vol. 59 (Winter, 1992), p. 3-7.
http://links.jstor.org/sici?sici=0162-2870%28199224%2959%3C3%3APOTSOC%3E2.0. CO%3B2-T.

[9] Byung-Chul H., *La sociedad de la transparencia,* Herder, Barcelona, 2013.

[10] *Vid.* Craig, T., y Ludloff, M., *Privacy and Big Data,* O'Really, 2011, Sebastopol (California), p. 4.

[11] *Vid.* McEwen, A., y Cassimally, H., *Internet de las cosas. La tecnología revolucionaria que todo lo conecta,* Anaya Multimedia, Madrid, 2014, p. 27.

[12] *Vid.* Swan, M., «Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0», *Journal of Sensor and Actuator Netwowoks,* núm. 1(3), p. 217-253, 2012. También, *Opinion 8/2014 on the on Recent Developments on the Internet of Things,* del Grupo de Trabajo del artículo 29, adoptado el 16 de septiembre de 2014.

[13] Bauman, Z., y Lyon, D., *Vigilancia líquida,* traducción de Alicia Capel Tejer, Paidós, Barcelona, 2013.

Como ha señalado Castells, en el último tercio del siglo xx se produce un cambio de paradigma[14] que afecta a todos los aspectos de la sociedad postindustrial. En la sociedad de la información o sociedad informatizada[15] «prima el "paradigma informacional" que conduce a una sociedad en la que la generación, el procesamiento y la transformación de información se convierten en las fuentes fundamentales de productividad y poder»[16]. Esta afirmación está más vigente que nunca; hoy la información es la materia prima y las tecnologías son para actuar sobre ella y nuestra existencia individual y colectiva está directamente modelada por la tecnología[17].

El propio medio digital fomenta la «exposición pornográfica de la intimidad y de la esfera privada»[18] y cada vez son mayores las posibilidades de reelaboración de esa información que los usuarios hacen disponible a través de la proliferación de «herramientas de comunicación y de expresión, dados los fenómenos de globalización e intercomunicación, habida cuenta de la posibilidad de "remixaje" y de bricolaje de todo lo que existe»[19]. Además, cuando navegamos por Internet dejamos rastros de forma inconsciente[20], que junto con otras herramientas y tecnologías formarían parte del conjunto de lo que ya ha sido denominado como el «panóptico digital»[21]. A los sistemas basados en la utilización de *cookies* o programas rastreadores o *sniffers*[22], que posibilitan el funcionamiento de las denominadas *redes de seguimiento* a través de las cuales es posible seguir al usuario a medida que navega por la red, hay que sumar actualmente las tecnologías *fingerprinting,* que

---

[14] Castells, M., *La era de la información,* Alianza Editorial, tercera edición, Madrid, 2008, pp. 103 ss.

[15] Frosini, V., *Il guirista e le tecnologie dell'informazione,* seconda edizione, Bulzoni Editore, Roma, 2000, p. 79.

[16] Marí Sáez, V. M., *Globalización, nuevas tecnologías y comunicación,* Ediciones de la Torre, Madrid, 1999, p. 34.

[17] Castells, M., *La era de la información,* ob. cit., pp. 103 ss.

[18] Byung-Chul H., *En el enjambre,* Herder Editorial, Barcelona, 2014, p. 14.

[19] Cobo Romaní, C., y Pardo Kuklinski, H., *Planeta Web 2.0. Inteligencia colectiva o medios fast food, Grup de Recerca d'Interaccions Digitals,* Universitat de Vic-Flacso México, Barcelona/México DF, 2007, p. 21.

[20] *Vid.* Recomendación 3/97, del el 3 de diciembre de 1997, sobre El anonimato de Internet; Dictamen 4/2012, de 7 de junio de 2012, sobre La exención del requisito de consentimiento de *cookies* y Dictamen 9/2014, de 25 de noviembre de 2014, sobre La aplicación de la Directiva 2002/58 a la identificación de dispositivos del Grupo de Trabajo del artículo 29.

[21] Byung-Chul H., *La sociedad de la transparencia,* ob. cit., p. 89.

Vid. Gandy, O. H., *The Panoptic Sort: A Political Economy of Personal Information,* Boulder, CO, Westview Press, 1993. Asimismo, Norris, C., «From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control», en Lyon, D. (ed.), *Surveillance as Social Sorting,* Routledge, Londres y Nueva York, 2005, o Reiman, J. H., «Driving to the panopticon: a philosophical exploration of the risks to privacy posed by highway technology of the future», en Barendt, E. (ed.); *Privacy*, Dartmouth Publishing Company, Aldershot, 2001.

[22] *Vid.* Téllez Aguilera, A., *Nuevas tecnologías, intimidad y protección de datos,* Edisofer, Madrid, 2001, pp. 83 ss.

permite «una recopilación sistemática de información sobre un determinado dispositivo remoto con el objetivo de identificarlo, singularizarlo y, de esta forma, poder hacer un seguimiento de la actividad del usuario del mismo con el propósito de perfilarlo»[23]. Nuestro rastro digital puede reunirse e interrelacionarse, con la consiguiente «transformación de datos en principio irrelevantes en un perfil peligrosamente público del ciudadano»[24]. La problemática derivada del tratamiento de este tipo de datos personales se complica también porque se trata de «datos invisibles» para el usuario de la red, cuyo almacenamiento o elaboración escapan a su conocimiento y a su control[25].

La cantidad de información personal disponible nos sitúa por sí misma ante una nueva revolución tecnológica, el *big data,* que «no se cifra en las máquinas que calculan los datos, sino en los datos mismos y en cómo los usamos»[26]. Pues, no solo es relevante a efectos del rastro digital, el tipo de información que ponemos a disposición de otros en Internet, sino que otro factor importantísimo es el de su cantidad, que va suponer por sí mismo un nuevo tipo de riesgo para los derechos. Los avances en la minería y análisis de datos y el aumento masivo de la capacidad informática de procesamiento y almacenamiento han ampliado exponencialmente la información que se encuentra al alcance de las empresas, los gobiernos y los individuos. Asimismo, el número creciente de gente, dispositivos y sensores que están conectados por redes digitales ha revolucionado la capacidad de generar, comunicar, compartir y acceder a los datos[27]. Denominamos *big data*, por un lado, a la gran cantidad de datos disponibles y, por otro, aludimos al conjunto de tecnologías cuyo objetivo es tratar grandes cantidades de información[28], empleando complejos algoritmos y estadística con la finalidad de hacer predicciones, extraer información oculta o correlaciones imprevistas y, en último término, favorecer la toma de decisiones. Para analizar estas inmensas cantidades de datos han surgido un conjunto de técnicas que hacen referencia a los sistemas de información y «que pertenecen al campo de la inteligencia artificial

---

[23] Estudio *fingerprinting* o Huella digital del dispositivo de la Agencia Española de Protección de Datos, p. 4. En: https://www.aepd.es/media/estudios/estudio-fingerprinting-huella-digital.pdf. Consultado el 16 de febrero de 2019.

[24] Drummond, V., *Internet, privacidad y datos personales,* traducción de I. Espín Alba, Editorial Reus, Madrid, 2004, p. 118.

[25] *Vid.* Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, aprobada por el Grupo de Trabajo el 23 de febrero de 1999.

[26] Mayer-Schönberger, V., y Cukier, K., *Big data. La revolución de los datos masivos,* Turner Noema, 2013, p. 18.

[27] Tene, O., y Polonetsky, J., «Privacy in the age of Big Data: a time for big decisions», *Stanford Law Review Online,* núm. 63, febrero de 2012, p. 63.

[28] Beltrán Pardo, M., y Sevillano Jaén, F., *Cloud computing, tecnología y negocio, P*araninfo, Madrid, 2013, pp. 16 ss.

(y) recibe el nombre de "minería de datos"»[29] y que, utilizando la ingente cantidad de datos disponibles los analizan buscando patrones recurrentes y correlaciones. Pero el *big data* es algo más. Puede ser definido como un fenómeno cultural, tecnológico y académico, que se apoya en la interacción de la tecnología a través de la maximización de la potencia de cálculo y precisión algorítmica y que utiliza estos análisis para identificar patrones en esos grandes volúmenes de datos, que sirven hacer reivindicaciones económicas, sociales, técnicas y legales; pero también aportaría un elemento mitológico, entendido como la creencia generalizada de que los grandes conjuntos de datos ofrecen una forma superior de la inteligencia y que su conocimiento puede generar ideas que antes eran imposibles, con el aura de la verdad, la objetividad y la precisión[30]. Es, precisamente este aura de objetividad y verdad, unida a la falta de transparencia que acompaña a las decisiones basadas en esta tecnología, lo que plantea más problemas para los derechos de las personas[31].

El *big data* es alimentado por la propia interacción de los usuarios de los servicios de Internet. Como se ha explicado, la navegación a través de Internet deja un rastro digital que permite monitorear las actividades de las personas en la red con el objetivo de elaborar un detallado perfil sobre cada usuario. De los servicios de Internet, dos son los que nos interesan particularmente: los motores de búsqueda y las redes sociales. Tanto los unos como los otros pueden suponer un impacto en determinada medida en los derechos de las personas, no solo por la gran cantidad de datos que sobre los usuarios recogen estos servicios[32], sino también por las posibilidades de utilizarlos para elaborar perfiles combinando e interrelacionando los datos personales obtenidos por varias vías. «Los buscadores nos siguen y almacenan enormes cantidades de información sobre nosotros»[33], sin que seamos

---

[29] Ramos Bernal, A., *Reflexiones sobre economía cuántica,* ECU (editorial Club Universitario), Alicante, 2012, p. 186.

[30] Boyd, D., y Crawford, K., «Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon», *Information, Communication & Society,* vol. 15, número 5, junio de 2012, pp. 662 y 663.

[31] *Vid.* O'neil, C., *Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia,* Capitán Swing, Madrid, 2017. Cathy O'Neil analiza el impacto real que han tenido en la vida de millones de personas los algoritmos predictivos basado en *big data* en campos tan diferentes como la prevención de la delincuencia, la contratación y los despidos de trabajadores, o su papel en la crisis económica de 2008.

Vid., asimismo, Monasterio Astobiza, A., «Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos», *Dilemata,* año 9 (2017), núm. 24, pp. 185-217.

[32] Explica Eli Pariser como desde diciembre de 2009 Google utilizaría 57 indicadores *«para conjeturar quién eres y qué clase de páginas te gustan»*. En Pariser, E., *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos,* Taurus, Barcelona, 2017, pp. 11 y 12.

[33] Suárez Ocaña, A., *Desnudando a Google. La inquietante realidad que no quieren que conozcas,* Planeta, Barcelona, 2012, pp. 253 ss.

conscientes de ello[34]. El Tribunal de Justicia de la Unión Europea, en relación con Google, ha señalado que los motores de búsqueda, «al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica», recogen datos personales «que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores» 35. Los usos de esta información pueden ser varios. Por ejemplo Google, «a partir de los terabytes de datos sobre comportamiento humano que recogen con su motor de búsqueda y otros sitios web (…) lleva a cabo millones de experimentos diarios, cuyos resultados utiliza para afinar sus algoritmos, que guían cada vez más nuestra manera de encontrar información y de extraer significado de ella» 36. Otros usos posibles son las de ofrecer publicidad a medida del usuario en función de sus intereses y preferencias detectadas a partir de su rastro digital.

Las redes sociales son servicios que ofrecen medios de interacción entre los usuarios basados en los perfiles que estos mismos generan, formándose comunidades de personas que comparten determinados intereses de tipo profesional o personal, sobre actividades o aficiones, etc. Y junto con la información personal publicada en línea por el propio usuario, registran la relativa a sus acciones, nuestro estado de ánimo[37], interacciones y reacciones a los distintos estímulos a los que son expuestos[38]. El usuario de las redes sociales asume un doble papel, el de consumidor y el de creador y, de esta forma «son los propios usuarios los que crean una gran base de datos cualitativos y cuantitativos, propios y ajenos con información relativa a edad, sexo, localización e intereses»[39]. La combinación de estos datos que el usuario aporta sobre el mismo y sobre terceros permite la obtención de un perfil muy preciso de sus intereses y actividades y estos datos o el resultado de su procesamiento podrán ser utilizados con distintos fines, sobre todo comerciales y de publicidad[40]. Estos servicios tecno-

---

[34] *Vid.* Dictamen 1/2008 del Grupo de Trabajo del artículo 29, sobre Cuestiones de protección de datos relacionadas con motores de búsqueda, de 4 de abril de 2008.

[35] Sentencia de 13 de mayo de 2014 (Asunto C-131/12). TJCE 2014\85.

[36] Carr, N., «¿Qué está haciendo Internet con nuestras mentes?», *Superficiales,* Taurus Pensamiento, Madrid, 2011, p. 184 y 185.

[37] A través de la informaciones que los usuarios suben a las redes sociales es posible hacer gráficas de sus emociones, sentimientos y estados de ánimo. Por ejemplo, Twitter «permite la datificación de pensamientos, estados de ánimo e interacciones de la gente» y ha llegado a acuerdos con dos empresas para comercializar el acceso a esos datos. En Mayer-Schönberger, V., y Cukier, K., *Big data. La revolución de los datos masivos,* ob. cit., pp. 116 y 117.

[38] Se explica con detalle en Lanier, J., *Diez razones para borrar tus redes sociales de inmediato,* Editorial Debate, Barcelona, 2018.

[39] Ortiz López, P., «Redes sociales: funcionamiento y tratamiento de información personal», en Rallo Lombarte, A., y Martínez Martínez, R. (coord.); *Derecho y redes sociales,* Civitas, Madrid, 2010, p. 24.

[40] *Vid.* Resolución sobre Protección de la privacidad en los servicios de redes sociales aprobada en Estrasburgo, los días 15 a 17 de octubre de 2008 en la 30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad.

lógicos se caracterizan porque se ofrecen bajo la falsa creencia de que se trata de un servicio gratuito, cuando realmente estos servicios se financian sobre todo a través de la utilización secundaria de los datos personales comercializándolos con fines de marketing personalizado, puesto que la información obtenida a través de las redes sociales y por los buscadores «es susceptible de ser utilizada para ofrecer publicidad basada en personas e intereses de una manera muy efectiva»[41], ya que pueden inferir otra mucha información sobre nosotros, incluso sensible. Por ejemplo, se puede inferir la orientación sexual del usuario, incluso en el caso de los denominados «perfiles en la sombra», relativos a personas que no tienen cuenta en una red social[42], o su perfil ideológico, económico, etc. El uso de la información personal de motores de búsqueda y redes sociales es la de proporcionar información relevante para mejorar la eficacia de la publicidad en línea; «la información es un producto: los datos "crudos", sin procesar no son aún información»[43] pero son la base de la mercancía final que resulta del procesamiento de los datos personales para convertirlos en un producto terminado. La publicidad comportamental *online*[44] se basa «en conocer los hábitos de comportamiento del consumidor en la red con el propósito de ofrecerle publicidad personalizada»[45]. La publicidad comportamental se basa en la observación continuada del comportamiento de los individuos para desarrollar un perfil específico, que permite proporcionar anuncios a medida de los intereses deducidos del comportamiento del usuario. A través del análisis de cada individuo, los anunciantes podrán dirigir a ese usuario «aquella publicidad que coincida con los gustos e intereses deducidos de dicho rastreo y análisis, incrementando así su eficacia»[46]. Internet, junto con las técnicas de publicidad basadas en el contexto o en los términos de búsqueda, «permite una verdadera personalización de la publicidad, mediante técnicas que tienen en cuenta información específica sobre el usuario concreto que está accediendo a un determinado sitio web»[47]. Como señala Javier Echeverría, al entrar en la caverna digital, pagamos un peaje publicitario, más o menos explícito y las empresas distribuyen

---

[41] Suárez Sánchez-Ocaña, A., *Desnudando a Google,* ob. cit., p. 252.

[42] Sarigol, E., García, D., y Schweitzer, F., «Online Privacy as a Collective Phenomenon», *Proceedings of the second edition of the ACM conference on Online social networks, ACM,* octubre de 2014, p. 105. Puede consultarse en: http://arxiv.org/pdf/1409.6197.pdf.

[43] Whitaker, R., *El fin de la privacidad,* Paidós, Barcelona, 1999, p. 94.

[44] *Vid.* el Dictamen 2/2010 sobre Publicidad comportamental del Grupo de Trabajo del artículo 29, adoptado el 22 de junio de 2010.

[45] Martínez Pastor, E., «La publicidad comportamental online y la protección de los datos personales», en Valero Torrijos, J., *La protección de los datos...,* ob. cit., p. 291.

[46] *Ibidem*.

[47] Peguera Poch, M., «Publicidad online basada en comportamiento y protección de la privacidad», en Rallo Lombarte, A. y Martínez Martínez, R. (Coord.), *Derecho y redes sociales,* ob. cit., p. 359.

gratuitamente productos tecnológicos sofisticados porque han conseguido seducir a tantos usuarios, tienen su modelo de negocio basado en los anuncios[48].

Esta inmensa capacidad para buscar, agregar y realizar referencias cruzadas de los grandes conjuntos de datos[49], que permiten extraer patrones de comportamiento y perfiles personales y que informan acerca de lo que somos y lo que hacemos[50] hace posible una peligrosa y nueva filosofía de la anticipación, cuyo extremo sería el de las predicciones preventivas[51]. Una de las consecuencias de la publicidad comportamental o dirigida es que puede influir en los deseos de nuevas maneras, pero también puede mediar en los comportamientos reales de ciertos grupos sociales que, como los individuos, son alentados por retroalimentación para ajustarse a los patrones esperados[52]. La libertad de elección y decisión de los individuos se verá directamente afectada, en la sociedad de consumo, sociedad sinóptica de adictos compradores/espectadores, «la obediencia al estándar (…) tiende a lograse por medio de la seducción, no de la coerción… y aparece bajo el disfraz de la libre voluntad, en vez de revelarse como una fuerza externa»[53]. Obviamente, cuanto más información se recabe sobre una persona y más preciso sea su perfil, más fácil será tentar y seducir sobre todo porque quienes controlan la información saben más de algunas personas que ellas mismas. Además, «la exploración de los datos hace visibles modelos colectivos de comportamiento de los que ni siquiera somos conscientes como individuos»[54] y, así, el procesamiento de la información sobre personas posibilita su clasificación social y la adopción de determinadas decisiones que le afectan.

III. PLATAFORMAS SOCIALES, MICROSEGMENTACIÓN *(MICROTARGETING)* Y MANIPULACIÓN EN LÍNEA

La interacción social se produce de forma más frecuente en los medios digitales[55]. Son muy pocas las empresas tecnológicas que

---

[48] Echeverría, J., *Entre cavernas. De Platón al cerebro pasando por Internet,* Triacastela, Madrid, 2013, p. 173.

[49] Boyd, D., y Crawford, K., *Critical questions for Big Data…,* ob. cit., p. 662.

[50] Craig, T., y Ludloff, M. E., *Privacy and Big Data,* ob. cit., p. 6.

[51] Kerr, I., y Earle, J., *Prediction, preemption, presumption: how Big Data threatens big picture privacy,* Stanford Law Review, *online* 65, septiembre de 2013.

[52] Lyon, D., *Surveillance Studies. An overview,* Polity Press, Malden, 2014, p. 101.

[53] Bauman, Z., *Modernidad líquida,* Fondo de Cultura Económica, Buenos Aires, 2013, p. 92.

[54] Byung-Chul H., *En el enjambre,* ob. cit., p. 109.

[55] Las redes sociales han experimentado un crecimiento enorme, ha aumentado el número de los usuarios activos (+9 %), de los que acceden a través del teléfono móvil (+10 %), y se ha incrementado el tiempo que medio que pasan en las redes sociales

aglutinan a la mayoría de los usuarios[56] por lo que operan en un sistema de cuasi-monopolio[57] y, por su volumen de negocio, destacan dos: Google y Facebook[58], que reúnen a millones de usuarios activos y «controlan más de la mitad del marketing online»[59]. Una de las consecuencias del rápido crecimiento de las redes sociales ha sido el aumento espectacular de las actividades maliciosas, como el *spam*, la creación de cuentas falsas, el *phishing* o la distribución de *malware*[60].

Las redes sociales son servicios basados en la web que permiten a los individuos construir un perfil público o semipúblico dentro de un sistema delimitado, articular una lista de otros usuarios con los que comparten una conexión y recorrer su lista de conexiones y las realizadas por otros dentro del sistema. Estos servicios reúnen información sobre los contactos sociales de los usuarios, construyen una gran red social interconectada y revelan a los usuarios cómo se conectan con los demás en la red[61]. Ahora bien, el perfil o una cuenta en una red social «no es propiedad del usuario, es un espacio puesto a su disposición gratuitamente, a cambio de su disponibilidad a ser seccionado en partes comercialmente interesantes»[62] y, como señala Bauman, en este ámbito, la socialización sigue las pautas del marketing y las herramientas electrónicas de la socialización digital «están hechas a la medida de las técnicas de marketing»[63]. Las prácticas del marketing comportamental clasifica a los individuos en función de su valor económico o su potencial como posibles compradores[64] o como consumi-

---

(actualmente es de 2 horas y 16 minutos). La red social con más usuarios activos sigue siendo Facebook a pesar de los continuos escándalos que le afectaron en el último año con 2.271 millones, que estaría seguida de YouTube con 1.900 millones. Igualmente la audiencia publicitaria creció un 4% en los tres últimos meses de 2018 hasta alcanzar los 895 millones de usuarios activos en todo el mundo. En España el orden de preferencia se altera ligeramente, siendo las redes sociales preferidas por lo españoles: YouTube (89 %), WhatsApp (87 %), Facebook (82 %), Instagram (54 %) y Twitter (49 %). Todos los datos son del informe Digital in 2019: Global Internet use accelerates. https://wearesocial.com/global-digital-report-2019 (consultado el 12 de febrero de 2019).

[56] Los Gafa: Google, Apple, Facebook y Amazon. *Vid.*, entre otros, Cardon, D., *Con qué sueñan los algoritmos. Nuestras vidas en el tiempo de los* big data, Dado ediciones, Madrid, 2018, p. 23.

[57] *Vid.* Moreno Muñoz, M., «Mediación tecnológica de la interacción social y riesgos de su instrumentalización. El caso de la plataforma Facebook», *Gazeta de Antropología,* 2018, núm. 34 (2), p. 1.

[58] A quien pertenecerían, entre otras, WhatsApp e Instagram.

[59] Sampedro Blanco, V., *Dietética digital. Para adelgazar al Gran hermano,* Icaria, Navarra, 2018, p. 64.

[60] Adewolea, K. S., Anuara, N. B., Kamsina, K., Varathana, K. D., y Razakb, S. A., «Malicious accounts: Dark of the social networks», *Journal of Network and Computer Applications* 79 (2017), p. 41.

[61] *Ibidem*, p. 43.

[62] Ippolita, En el acuario de Facebook. El irresistible ascenso del anarco-capitalismo, Enclave de Libros, Madrid, 2012, p. 64.

[63] Z. Bauman, *Vida de consumo,* Fondo de Cultura Económica, Madrid, 2007, p. 157.

[64] *Vid.* O. H. G., *The Panoptic Sort: A Political Economy of Personal Information,* ob. cit.

dores fallidos[65]. La industria digital «hace de la comunicación social un negocio y la transforma en publicitaria»[66]. Por esta razón uno de los primeros objetivos que han de lograr las plataformas sociales es la fidelización de los usuarios, consiguiendo que éstos pasen el mayor tiempo posible en sus servicios. Para conseguir sus objetivos económicos las plataformas sociales diseñan su arquitectura y herramientas de formas muy concretas y este diseño fabrica nuestra realidad, la organiza y la orienta[67]. Explica Lanier, que la información personal recolectada sirve para que los algoritmos establezcan correlaciones entre los datos de un mismo individuo y entre los de otras personas diferentes, constituyendo teorías sobre la naturaleza de cada persona midiendo y clasificando continuamente respecto de su predictibilidad y, posteriormente, «los algoritmos deciden lo que cada persona experimenta a través de sus dispositivos»[68].

La comercialización de los datos personales constituye el aspecto principal de su modelo de negocio. En su Dictamen 5/2009 sobre las redes sociales en línea, el Grupo de Trabajo del artículo 29 identificó varias formas de comercialización de los datos de los usuarios: la directa; la contextual, que se adapta al contenido visto por el usuario o al que accede; la segmentada, que consiste en difundir publicidad a grupos de usuarios específicos definidos en función de una pluralidad de criterios y ordenados según la información que han comunicado directamente a la red social y la comercialización del comportamiento, que «selecciona la publicidad basándose en la observación y análisis de la actividad del usuario a lo largo del tiempo»[69].

La evolución del proceso de segmentación de mercados en marketing ha supuesto el paso de la segmentación por grupos, socio-geográfica, por ejemplo a través del código postal, a la segmentación de individuos a través de las técnicas de *microtargeting*. Éste puede definirse como una segmentación psicográfica avanzada que se basa en un algoritmo que determina una serie de rasgos demográficos y de actitud que permite distinguir a cada individuo para cada segmento objetivo y que permite hacer predicciones precisas de la reacción de la audiencia objetiva[70]. La cantidad y calidad de la información personal que se encuentra en las redes sociales, permite a los anunciantes mejorar el alcance e impacto de su publicidad al dirigirse a grupos específicamente seleccionados y estructurados o, incluso, a individuos con-

---

[65] Z. Bauman, *Vida de consumo,* ob. cit., p. 82.

[66] Sampedro Blanco, V., *Dietética digital,* ob. cit, p. 65.

[67] Cardon, D., *Con qué sueñan los algoritmos. Nuestras vidas en el tiempo de los big data,* Dado ediciones, Madrid, 2018, p. 21.

[68] Lanier, J., *Diez razones para borrar tus redes sociales de inmediato,* ob. cit., p. 47.

[69] Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009, p. 10.

[70] Barbu, O., «Advertising, Microtargeting and Social Media», *Procedia-Social and Behavioral Sciences* 163 (2014), pp. 44-45.

cretos para influir en su conducta[71]. Obviamente, estas técnicas pueden utilizarse para vender un producto determinado, pero también para favorecer una determinada ideología. El uso de perfiles permite determinar la información a la que vamos a tener acceso, limitando también nuestro derecho a recibir información veraz o siendo objeto de auténticas manipulaciones. A través de los distintos algoritmos utilizados por las plataformas sociales unos usuarios tienen acceso a un tipo de información y otros, en función de sus intereses o de su perfil ideológico[72], a otros contenidos diferentes. Estos servicios utilizan algoritmos que personalizan las noticias u otros contenidos para cada usuario, ya que «los parámetros de medición basados en afinidades digitales delimitan, para el usuario, ventanas de visibilidad que tienen el color de su red social»[73], aunque pueden suponer también que no se vea expuesto a informaciones que no encajen con su ideología. A través de los hilos de contenido personalizado, que se optimizan para captar a cada usuario, «a menudo utilizando potentes estímulos emocionales que conducen a la adicción a las personas»[74], se las puede manipular sin que sean conscientes de ello[75]. Se trata de modelos de negocio que basan sus ingresos en la venta de publicidad y por lo tanto necesitan captar la atención del usuario por lo que los algoritmos utilizados priorizarán aquellos contenidos que consigan este objetivo de forma más eficiente y el incremento de esta atención se consigue mejor a través de la amplificación de las emociones negativas frente a las positivas[76].

En este contexto y en la medida en que la exposición a noticias, opiniones e información cívica ocurre cada vez más a través de las redes sociales[77], los agentes políticos se ven compelidos a utilizar también estos medios, por su eficacia y para conseguir una mayor visibilidad[78]. Ahora bien, no es lo mismo el debate de ideas o la publi-

---

[71] *Ibidem*, p. 46.

[72] *Vid.* Bakshy, E., Messing, S., y Adamic, L. A., «Exposure to ideologically diverse news and opinion on Facebook», *Science,* junio de 2015, vol. 348, núm. 6239, p. 1130-1132.

[73] Cardon, D., *Con qué sueñan los algoritmos,* ob. cit., p. 43.

[74] Lanier, J., *Diez razones para borrar tus redes sociales de inmediato,* ob. cit., p. 48.

[75] En ocasiones, bajo la coartada del experimento sociológico, se realiza sin tapujos una directa manipulación emocional de los usuarios. A lo largo de una semana durante el año 2012, Facebook experimentó con 689.000 usuarios sin su consentimiento para analizar su comportamiento alterando el algoritmo que selecciona las noticias que se ven de los amigos y, a través del tipo de noticias que mostraba a unos u a otros, positivas o negativas, para estudiar como influía en su estado de ánimo. En Kramer, A., Guillory, J. E., y Hancock, J. T., «Experimental evidence of massive-scale emotional contagion through social networks», *Proceedings of the National Academy of Sciences of Unites States of America,* vol. 11, núm. 24, marzo de 2014.

[76] Lanier, J., *Diez razones para borrar tus redes sociales de inmediato,* ob. cit., p. 42.

[77] Bakshy, E., Messing, S. y Adamic, L. A., *Exposure to ideologically*…, ob. cit., p. 1130.

[78] Sobre esta cuestión *vid.* Echeverría, J., *Entre cavernas,* ob. cit., especialmente pp. 175 ss.

cidad legítima, que la propagación de noticias falsas y los fenómenos de desinformación que utilizan el potencial del *big data* y de la microsegmentación para conseguir sus objetivos económicos o políticos. En su informe «Disinformation and "fake news": Final Report», del 14 de febrero de 2019, el Parlamento Británico concluía que, la proliferación de daños en Internet se hace más peligrosa al centrar mensajes específicos en los individuos como resultado de la «micro-mensajería dirigida», que a menudo se aprovecha y distorsiona la visión negativa de las personas sobre sí mismas y sobre los demás[79].

El fenómeno de las noticias falsas es complejo[80] y es posible distinguirlas de un variado elenco de situaciones posibles que abarcarían desde las teorías de la conspiración hasta las informaciones erróneas pasando por las noticias de los medios de comunicación sesgados ideológicamente[81]. Lo que caracteriza a las *fake news* es que éstas son intencional y verificablemente falsas[82] y las empresas que las producen buscan el máximo beneficio a corto plazo para atraer el mayor número de «clics» y persiguen la viralización de la noticia y el aumento del tráfico en la red[83] «porque eso es lo que impulsa la influencia y los ingresos por publicidad»[84]. Este fenómeno se ve potenciado porque su contenido puede ser retransmitido entre los usuarios sin necesidad de un filtrado de verificación de hechos o juicio editorial significativo por parte de terceros, aprovechándose también del incentivo psicológico que supone el sesgo de confirmación[85]. Por la complejidad del fenómeno, tanto el Parlamento británico como la Comisión Europea[86], prefieren centrar el debate sobre el problema de la desin-

---

[79] «Disinformation and "fake news": Final Report», p. 11 (consultado el 1 de marzo de 2019). https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

[80] A la desinformación contribuyen no solo las noticias falsas, sino también las cuentas falsas y *bots* «que amplifican la actividad e intensidad de los servicios». Lanier, J., *Diez razones para borrar…*, ob. cit., p. 77.

[81] Alcott, H., y Gentzkow, M., «Social Media and Fake News in the 2016 Election», *Journal of Economic Perspectives,* volumen 31, núm. 2, 2017, p. 217 ss.

[82] *Ibidem*, p. 213.

[83] Esta tendencia no es exclusiva de quienes distribuyen este tipo de información. También las empresas tradicionales de comunicaciones buscan titulares y noticias que se hagan virales y «en su afán por adaptar su modelo de negocio para Internet, a partir de pautas publicitarias generadas por trafico, se ven abocados a la preocupación por las estadísticas de sus portales» (Lotero-Echeverri, G., Romero-Rodríguez, L. M., Pérez-Rodríguez, M. A., «Fact-checking vs. Fake news: Periodismo de confirmación como recurso de la competencia mediática contra la desinformación», *index. comunicación,* núm. 8(2), 2018, p. 298.

[84] Holiday, R., *Confía e mi, estoy mintiendo. Confesiones de un manipulador de los medios,* Empresa Activa, Barcelona, 2013, pp. 290-291.

[85] Alcott, H., y Gentzkow, M., «Social Media and Fake News in the 2016 Election», *Journal of Economic Perspectives,* ob. cit., p. 211.

[86] Final report of the High Level Expert Group on Fake News and Online Disinformation: «A multi-dimensional approach to disinformation» (12 de marzo de 2018). https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (consultado el 17 de octubre de 2018).

formación, el resultado, que sobre los medios, las noticias falsas. La desinformación incluiría la información inexacta, engañosa o falsa que ha sido diseñada y promovida para causar intencionalmente un daño (entre los que se puede incluir la amenaza a los procesos y valores democráticos, incluidas las elecciones) o con fines de lucro, que puede ser exacerbada por la forma en que el público y las comunidades reciben, se involucran y amplifican la desinformación[87].

IV. LA INTERDEPENDENCIA ENTRE LOS DERECHOS A LA PROTECCIÓN DE DATOS PERSONALES, LA LIBERTAD DE EXPRESIÓN Y LA LIBERTAD IDEOLÓGICA

El escándalo Facebook-Cambridge Analytica evidenció una serie de prácticas que habrían afectado, al menos, a 50 millones de personas y sobre cuyos datos personales almacenados por Facebook se habrían elaborado perfiles individuales con fines de micro-marketing político en la elecciones presidenciales de Estados Unidos de 2016 y en el referéndum sobre la permanencia en la Unión Europea del Reino Unido[88]. En 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, se considera constatado que las fugas de datos de usuarios y el acceso concedido a aplicaciones de terceros sirvieron para utilizarse indebidamente en campañas electorales[89].

No es este un problema nuevo para las autoridades de protección de datos, que en el año 2005 adoptaron una Resolución sobre el usos de datos personales para la comunicación política[90] poniendo de manifiesto la existencia de la realización invasiva de perfiles de personas, que las clasifica como simpatizantes, partidarios, adherentes o miembros de un partido, para intensificar la comunicación personalizada con grupos de ciudadanos. Para ello, las organizaciones políticas recopilarían una gran cantidad de datos personales que incluiría, además de los datos de contacto, informaciones sobre su actividad profesional y relaciones familiares, «datos sensibles relacionados con convicciones o actividades políticas o morales reales o supuestas, o con actividades de votación». Pero, si bien este no es un problema nuevo,

---

[87] *Ibidem*, p. 10.

[88] De forma detallada se recogen en el Informe de la Cámara de los Comunes de 14 de febrero de 2019 «Disinformation and "fake news": Final Report».

[89] *Vid.* Considerando A de 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)].

[90] Resolución sobre el Uso de Datos Personales para la Comunicación Política de las Autoridades de Protección de datos, adoptada en la Conferencia de Montreaux del 14 al 16 de septiembre de 2005.

lo cierto es que las posibilidades actuales de micro-segmentación y manipulación *online* basadas en las tecnologías de *big data* e inteligencia artificial que permiten la recolección, el almacenamiento, la combinación y el análisis de ingentes cantidades de datos personales hacen que el riesgo para los derechos de las personas sea hoy mucho más real y elevado. Como ha señalado el Supervisor Europeo de Protección de Datos existe una amenaza para los valores democráticos y los derechos fundamentales derivados de la incesante vigilancia a la que son sometidas las personas en el espacio digital por empresas y Estados y, esta disminución de su espacio íntimo tiene como consecuencia «un efecto alarmante sobre la capacidad y voluntad de las personas de expresarse y establecer relaciones con libertad, también en la esfera cívica, tan esencial para la salud de la democracia»[91].

Existe una relación de interdependencia entre el derecho a la vida privada y las libertades de expresión e ideológica. El derecho a la protección de datos personales cumple una importante función de garantía de otros derechos fundamentales como reiteradamente ha destacado el Tribunal Constitucional[92]. El tratamiento de los datos relativos a cualquier persona puede «servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier índole, o (…) para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo»[93]y, precisamente, es esta capacidad para la elaboración de perfiles predictivos cada vez más precisos y detallados, que va a permitir el envío de mensajes publicitarios y políticos diseñados específicamente, dirigidos y personalizados para grupos de personas cada vez más y mejor segmentadas, lo que podría poner en riesgo, a través de campañas de desinformación basadas en estos perfiles, las libertades de expresión e información.

Las libertades de expresión e información son dos derechos diferentes, la primera «tiene por objeto la expresión de pensamientos, ideas y opiniones, concepto amplio dentro del que deben incluirse también las creencias y las creencias y juicios de valor» [94]. El derecho-deber a la información veraz garantiza el derecho a comunicar y recibir libremente información «sobre hechos que puedan considerarse noticiables»[95]. Dada la cuestión de la que nos estamos ocupando, conviene recordar que, de acuerdo con su configuración constitucional, la exigencia de veracidad actúa como límite interno de la libertad de información, pues la propia constitución configura la libertad de

---

[91] Opinion 3/2018, on online manipulation and personal data, del Supervisor Europeo de Protección de Datos, adoptada el 13 de marzo de 2018, p. 3.

[92] SSTC 11/1998, de 13 de enero (RTC 1998\11); 33/1998, de 11 de febrero (RTC 1998/33); 35/1998, de 11 de febrero (RTC 1998/35); 45/1998 de 24 de febrero (RTC 1998/45); 104/1998, de 18 de mayo; 198/1998 (RTC 1998/198), de 13 de octubre o 44/1999, 22 de marzo (RTC 1999/44).

[93] STC 292/2000, de 30 de noviembre (RTC 2000/292).

[94] STC 6/1988, de 21 de enero (RTC 1988/6).

[95] *Ibidem*.

información como el derecho a transmitir información veraz, por lo que es una condición imprescindible para legitimar el ejercicio de esta libertad. No obstante, el requisito constitucional de veracidad no exige una rigurosa y absoluta exactitud en el contenido de la información[96], si bien se hace imprescindible una especial actitud del informador en orden a «comprobar la veracidad de los hechos que expone mediante las oportunas averiguaciones, y empleando la diligencia exigible a un profesional (…), excluyendo invenciones, rumores o meras insidias»[97].

Nota distintiva y especialmente relevante de ambas libertades es que son, además de derechos fundamentales, garantías institucionales, es decir, instrumentos de los que se vale el sistema democrático para protegerse[98]. La institución que garantizan es la opinión pública libre, fundamento del pluralismo político y elemento básico en un sistema democrático[99]. Las libertades de expresión y de información cumplen por ello una función esencial de preservación del principio democrático y del pluralismo ideológico al permitir a los ciudadanos formar sus propias opiniones y convicciones, su conciencia individual y colectiva acerca de hechos y acontecimientos, así como participar en la discusión social sobre asuntos de interés público. Además, sin la garantía institucional de la opinión pública, se podría «poner en tela de juicio la base organizativa jurídica y política de cualquier Estado democrático y no se garantizaría (…) la ineludible protección de las minorías, como mecanismo institucionalizado para garantizar la disidencia o la heterodoxia»[100]. En su dimensión objetiva, estas libertades actúan como elementos esenciales para establecer el necesario equilibrio entre poderes en las sociedades democráticas, contribuyen a realizar los fines del Estado porque son vehículos para la participación política y constituyen «un instrumento de control que tanto puede afectar al procedimiento de las tomas de decisiones como a la cualidad y legitimidad de las personas al frente de las instituciones políticas» 101. Por lo tanto, constituyen «una condición previa y necesaria para el ejercicio de otros derechos inherentes al funcionamiento de un sistema democrático (…). Para que el ciudadano pueda formar libremente sus opiniones y participar de modo responsable en los asuntos públicos,

---

[96] *Ibidem*.

[97] STC 105/1990, de 6 de junio (RTC 1990/105). En el mismo sentido SSTC 171/1990, de 12 de junio (RTC 1990/171); 197/1991, de 17 de octubre (RTC 1991/197); 85/1992, de 8 de junio (RTC 1992/85) o 148/2002, de 15 de julio (RTC 2002/148).

[98] *Vid.* Llamazares Calzadilla, M.ª C., *Las libertades de expresión e información como garantía del pluralismo político,* Civitas-Universidad Carlos III de Madrid, 1999, especialmente pp. 43 ss.

[99] STC 104/1986, de 17 de julio (RTC 1986/104). En el mismo sentido, entre otras, SSTC 12/1982, de 31 de marzo; 159/1986, de 12 de diciembre; 172/1990, de 12 de noviembre o 214/1991, de 11 de noviembre.

[100] Rodríguez García, J. A., *El control de los medios de comunicación,* Dykinson, Madrid, 1998, p. 10.

[101] Soriano, Ramón: *Las libertades públicas,* Tecnos, Madrid, 1990, p. 109.

ha de ser también informado ampliamente de modo que pueda ponderar opiniones diversas e incluso contrapuestas»[102]. Cuando la ciudadanía ejerce su derecho al sufragio elige sobre la base de un juicio que se construye sobre el conocimiento del que disponga de los asuntos públicos y su gestión. Y este conocimiento sobre asuntos de relevancia pública puede garantizar esa actuación libre de los ciudadanos pues, como nos recuerda el Tribunal Constitucional, «únicamente aquellas sociedades que pueden recibir informaciones veraces y opiniones diversas de cuanto constituyen los aspectos más importantes de la vida comunitaria, están en condiciones de ejercitar, después, sus derechos y cumplir sus deberes como ciudadanos, partiendo del principio esencial de que la soberanía nacional reside en el pueblo, del que emanan los poderes del Estado (art. 1.2 CE)»[103]. Las libertades de expresión e información encuentran por todas las razones anteriores su fundamento en la dignidad de la persona, la libertad de conciencia y el pluralismo político. Entre estos tres valores, que se implican mutuamente, se produce «una relación secuencial que se articula de la manera siguiente: el pluralismo político es condición *sine qua non* de la libertad de conciencia y, consecuentemente, de la dignidad personal»[104].

En período electoral todas las cuestiones anteriores y el papel que desempeñan las libertades de expresión e información es si cabe aún más relevante, pues como señala el Tribunal Europeo de Derechos Humanos (TEDH), la libertad de expresión, en particular la libertad de debate político, constituyen la base de todo sistema democrático[105]. Ambos derechos «están interrelacionados y se refuerzan mutuamente: por ejemplo, la libertad de expresión es una de las «condiciones» necesarias para «garantizar la libre expresión de la opinión del pueblo en la elección del poder legislativo» y, por ello, «es particularmente importante en el período anterior a una elección que se permita la libre circulación de opiniones e información de todo tipo. En el contexto de los debates electorales, el ejercicio sin trabas de la libertad de expresión por parte de los candidatos tiene especial importancia»[106].

La libre circulación de opiniones e informaciones se ve obstaculizada y, consiguientemente, el debate electoral, cuando se aplican «burbujas de filtro». Como ya he señalado, la recopilación masiva de datos personales permite elaborar un perfil preciso que servirá para que los algoritmos que utilizan los servicios de noticias establezcan correlaciones «de todo lo que hacemos con lo que hacen casi todos los

---

[102] STC 159/1986, de 16 de diciembre (RTC 1986/159). También SSTC 6/1981 de 16 marzo o 104/1986 de 17 julio.

[103] STC 173/1995, de 21 de noviembre (RTC 1995/173).

[104] Llamazares Calzadilla, M.ª C., *Las libertades de expresión*…, ob. cit., p. 47.

[105] SSTEDH de 2 de marzo de 1987, caso Mathieu-Mohin y Clerfayt c. Bélgica (TEDH 187/3) y de 8 de julio de 1986, caso Lingens c. Austria (TEDH 1986/8).

[106] STEDH de 21 febrero 2017, caso Orlovskaya Iskra c. Rusia (JUR 2017\44341).

demás» y se diseñan estímulos individualizados para modificar nuestra conducta[107]. La nueva generación de filtros de internet «son máquinas de predicción cuyo objetivo es crear y perfeccionar constantemente una teoría acerca de quién eres, lo qué harás y lo qué desearás a continuación»[108] formando una burbuja de filtros invisible, que nos aísla y que no elegimos. Además al desconocer la forma y los criterios según los cuales los servicios filtran la información que entra y sale, «es prácticamente imposible ver lo sesgada que es»[109]. Como consecuencia de ello, cuando el entorno *online* se encuentra personalizado y micro-segmentado, los ciudadanos estamos expuestos a informaciones que refuerzan los sesgos ideológicos y es más difícil encontrar opiniones diferentes, lo que lleva «a una mayor polarización política e ideológica»[110]. En este sentido, también el Parlamento Europeo[111] ha analizado los riesgo de la elaboración de perfiles utilizando *macrodatos* y, entre otras consideraciones, insta a la «Comisión y a los Estados miembros que velen por que las tecnologías basadas en los datos no limiten o discriminan el acceso a un entorno mediático pluralista sino que fomenten la libertad de los medios de información y el pluralismo». En su Informe de enero de 2018, el Grupo Consultivo sobre Ética del Supervisor Europeo de Protección de Datos[112] señalaba, entre las amenazas para la autonomía individual, la difusión algorítmica o humana de noticias falsas que debilita la capacidad de los individuos para discriminar entre lo que es información fiable y lo que no lo es y, así también, los procesos democráticos estarían en riesgo de debilitarse a través de las prácticas de marketing político basadas en técnicas de micro-segmentación y elaboración de perfiles psicográficos[113]; pues, las técnicas de micro-segmentación en el ámbito electoral cambia las reglas del discurso político, reduciendo el espacio para el debate y el intercambio de ideas[114].

También la libertad ideológica puede resultar afectada por las prácticas anteriormente descritas. Su papel es esencial en un Estado democrático y abarca «todas las opciones que suscita la vida personal y social (…) y para cuya efectiva realización es precisa la maduración intelectual en una mentalidad amplia y abierta»[115]. La libertad ideológica se encuentra estrechamente vinculada a la dignidad humana

---

[107] Lanier, J., *Diez razones para borrar*…, ob. cit., pp. 18-19.
[108] Pariser, E., *El filtro burbuja*…, ob. cit., p. 18.
[109] *Ibidem*.
[110] Opinion 3/2018, on online manipulation and personal data, del Supervisor Europeo de Protección de Datos, adoptada el 13 de marzo de 2018, p. 7.
[111] Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley.
[112] EAG; Report 2018: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf (consultado el 23 de noviembre de 2018).
[113] *Ibidem*, p. 18.
[114] *Ibidem*, p. 28.
[115] ATC núm. 40/1999 de 22 febrero (RTC 1999\40 Auto).

puesto que «otorga dimensión moral a la vida humana en el sentido de que, en función de las creencias profesadas, el individuo puede orientar libremente el sentido de su existencia que adquiere así, en cuanto libremente determinada, dimensión moral»[116]. Pero, además de fundamento de la autoderminación de la persona, la libertad ideológica es presupuesto del derecho de participación y del pluralismo político[117]. La relación de la libertad ideológica con el valor superior del pluralismo político tiene una doble dimensión que se concreta en la relación indirecta a través del valor libertad en la medida en que el pluralismo se configura como la dimensión política de la libertad; pero, asimismo existe una relación directa puesto que, «además de ser un valor fundamental, es también un requisito de funcionamiento del Estado democrático» 118. Señala el Tribunal Constitucional que «sin la libertad ideológica consagrada en el artículo 16.1 de la Constitución, no serían posibles los valores superiores de nuestro ordenamiento jurídico que se propugnan en el artículo 1.1 de la misma para constituir el Estado social y democrático de derecho que en dicho precepto se instaura» 119. La libertad ideológica, por ser esencial «para la efectividad de los valores superiores y especialmente del pluralismo político, hace necesario que el ámbito de este derecho no se recorte ni tenga "más limitación (en singular utiliza esta palabra el artículo 16.1 CE), en sus manifestaciones, que la necesaria para el mantenimiento del orden público protegido por la ley"»[120].

En nuestro sistema de valores, la ideología es una cuestión privada e íntima. Las ideas que se profesen, «cualesquiera que sean, no pueden someterse a enjuiciamiento, y nadie, como preceptúa el artículo 14 de la CE, puede ser discriminado en razón de sus opiniones»[121]. Esta dimensión de la libertad de conciencia nos remite al ámbito en el que se generan y forman nuestras creencias e ideas, al ámbito «de nuestra concepción personal sobre el mundo, la vida y la sociedad»[122]. Este rasgo situaría a la libertad de conciencia muy próxima al derecho a la intimidad y, para garantizarlo, el artículo 16.2 CE establece un elemento negativo al determinar que «nadie podrá ser obligado a declarar sobre su ideología, religión o creencias»[123]. Por lo tanto, el

---

[116] Rollnert Liern, G., «La libertad ideológica en la jurisprudencia del Tribunal Constitucional», *Cuadernos y Debates* núm. 129, Centro de Estudios Políticos y Constitucionales, Madrid, 2002, p. 66.

[117] Xiol Ríos, J. A., «La libertad ideológica o libertad de conciencia», en AA. VV., «La libertad ideológica. Actas e las VI Jornadas de la Asociación de Letrados del Tribunal Constitucional», *Cuadernos y Debates* n.º 115, Centro de Estudios Políticos y Constitucionales, Madrid, 2001, pp. 19 ss.

[118] Rollnert Liern, G., *La libertad ideológica en*…, ob. cit., p. 70.

[119] STC 20/1990 de 15 de febrero (RTC 1990\20).

[120] *Ibidem*.

[121] ATC 195/1983, de 4 de mayo.

[122] Martínez de Pisón Cavero, J., *Constitución y libertad religiosa en España,* Dykinson, Madrid, 2000, p. 305.

[123] STC 46/2001, de 15 de febrero (RTC 2001\46).

derecho fundamental a la libertad ideológica garantiza el derecho de las personas a manifestar sus opiniones políticas sin que por ello puedan ser discriminadas o limitado su ejercicio por los poderes públicos salvo que sea necesario para el mantenimiento del orden público, pero también supone el derecho a no revelar la propia ideología. Se trata de un derecho complejo con distintas facetas o dimensiones y que inicialmente el Tribunal Constitucional formuló conjuntamente de forma genérica para la libertad religiosa e ideológica[124]. En su dimensión externa, constituye «el reconocimiento de un ámbito de actuación constitucionalmente inmune a la coacción estatal» [125] y en su dimensión interna, representa el «derecho a adoptar una determinada posición intelectual ante la vida y cuanto le concierne y a representar o enjuiciar la realidad según personales convicciones»[126] y esta dimensión íntima o negativa de la libertad ideológica se concreta «por la determinación constitucional de que «nadie podrá ser obligado a declarar sobre su ideología, religión o creencias» (art. 16.2 CE)»[127]. Precisamente para garantizar este elemento negativo de la libertad ideológica y de conciencia, tanto el RGPD como la LOPDyGDD prohíben como regla general el tratamiento de los datos personales que revelen las opiniones políticas, las convicciones religiosas o filosóficas (arts. 9.1 de ambas normas). Ahora bien en el ámbito del *big data*, las posibilidades de elaboración de perfiles con el auxilio de la inteligencia artificial y el aprendizaje automático hace posible inferir las convicciones ideológicas y de conciencia de una persona sin que esta la haya hecho pública. Así lo señala el Grupo de Trabajo del artículo 29, ya que «pueden hallarse correlaciones que indiquen algo sobre la salud, las convicciones políticas, las creencias religiosas o la orientación sexual de las personas»[128]. Por tanto, en la medida en que a través de estas tecnologías es posible inferir la ideología de una persona se estaría conculcando el derecho fundamental del artículo16.2 CE y en el contexto de unas elecciones políticas, la elaboración de perfiles ideológicos para aplicar las técnicas de *microtargeting,* podría afectar también al derecho del artículo 23.1 CE. Estamos ante libertades ínti-

---

[124] Rollnert Liern, G., *La libertad ideológica en*…, ob. cit., p. 45 ss.

[125] STC 141/2000, de 29 de mayo (RTC 2000\141).

[126] Sentencia núm. 120/1990 de 27 junio (RTC 1990\120).

[127] Sentencia núm. 46/2001 de 15 febrero (RTC 2001\46).

[128] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 17. El Grupo de Trabajo recoge el estudio de Kosinski, M., Stilwell, D., y Graepel, T., «Private traits and attributes are predictable from digital records of human behaviour», *Proceedings of the National Academy of Sciences of the United States of America,* volumen 110, núm. 15, pp. 5802-5805. Dicho estudio, según se recoge por el Grupo del artículo 29, «combinó los "me gusta" de Facebook con información limitada procedente de encuestas y halló que los investigadores predijeron con exactitud la orientación sexual de un usuario varón en el 88 % de los casos; el origen étnico de un usuario en el 95 % de los casos; y si un usuario era cristiano o musulmán en el 82 % de los casos».

mamente relacionadas puesto que la libertad de expresión es el cauce que permite la manifestación y por tanto el ejercicio de la dimensión externa de la libertad ideológica[129]. Por otra parte, los derechos garantizados por el artículo 23 CE, que se encuentran íntimamente conectados formando un todo inescindible[130], «poseen, no solo un contenido prestacional y una función de garantía de institutos políticos, como el de la opinión pública libre, sino también un contenido de derecho de libertad, que se concreta, en lo que aquí interesa, en la posibilidad constitucionalmente protegida de ofrecer a los ciudadanos, sin interferencias o intromisiones de los poderes públicos, los análisis de la realidad social, económica o política y las propuestas para transformarla que consideren oportunas»[131]. Al igual que las libertades de expresión e ideológica los derechos de participación política permiten la efectiva realización de los valores superiores de nuestro Derecho, en especial la libertad y el pluralismo político y contribuyen a asegurar la formación de la opinión pública libre. Con estos derechos al igual que con las libertades de expresión y de comunicación, indica el Tribunal Constitucional, se persigue garantizar «a las personas que participan como actores en la actividad pública, y a los partidos y grupos en los que aquéllas se integran la posibilidad de contribuir a la formación y expresión de la opinión pública libre, poniendo a disposición de los ciudadanos en general y de los electores en particular una pluralidad de opciones políticas para que puedan formar sus propias opiniones políticas y, en el momento electoral, para que puedan elegir libremente los programas que estimen más adecuados»[132]. Al cumplir una función tan esencial en el sistema democrático «deberá garantizarse la máxima libertad –y los mayores medios– para que los individuos y los grupos hagan llegar a los electores cualquier tipo de opiniones o informaciones «para que el ciudadano pueda formar libremente sus opiniones y participar de modo responsable en los asuntos públicos» (…) pero, por el mismo motivo, en este contexto deberá existir una especial cautela respecto de todo aquello que pueda limitar la libertad de opción de los ciudadanos y, muy especialmente, durante los procesos electorales»[133].

La relación entre todos estos derechos fundamentales está clara. Todos ellos contribuyen a garantizar la institución de la opinión pública libre y ello requiere que no se introduzcan interferencias y manipulaciones, se permita acceder a informaciones veraces y compartirlas e incluso discutirlas sin que los filtros automáticos basados en el perfil ideológico individual limiten el alcance de las informaciones a los que

---

[129] STC 136/1999 de 20 julio (RTC 1999\136).

[130] STC 5/1983 de 4 febrero (RTC 1983\5) y STC 136/1999 de 20 julio (RTC 1999/136), entre otras.

[131] STC 136/1999 de 20 julio.

[132] *Ibidem*.

[133] *Ibidem*.

la ciudadanía va a tener acceso. Para el Tribunal Constitucional, serán los electores quienes habrán de decidir que mensajes quieren recibir y cuales no y el que valor le atribuyen a estos mensajes sin que los poderes públicos deban intervenir para acotar los mensajes electorales. Sin embargo podría producirse una intervención automática y opaca en la información que se recibe, sin los necesarios filtros que garanticen suficientemente su veracidad. Y si bien nuestro Tribunal Constitucional considera, que en el ámbito de los procesos electorales, solo en casos muy extremos cabría admitir «la posibilidad de que un mensaje tenga capacidad suficiente para forzar o desviar la voluntad de los electores, dado el carácter íntimo de la decisión del voto y los medios legales existentes para garantizar la libertad del sufragio», ya que frecuentemente los partidos políticos durante las campañas electorales suelen pronosticar «todo tipo de peligros y calamidades que necesariamente habrán de seguirse del triunfo de las opciones contrarias sin que ello pueda considerarse intimidatorio o amenazante»[134], como señala el Defensor del Pueblo[135], el actual contexto tecnológico ha cambiado las reglas del juego. Si bien es innegable que los mensajes alarmistas, xenófobos o el discurso del miedo no es una realidad que haya surgido con la sociedad digital, lo cierto es que la capacidad de manipulación que permiten las prácticas de micro-segmentación basadas en perfiles individuales eran fenómenos desconocidos hasta hoy.

V. LA ELABORACIÓN DE PERFILES Y EL NUEVO ARTÍCULO 58 BIS.1 DE LA LEY ORGÁNICA DE RÉGIMEN ELECTORAL GENERAL[136]

Antes de examinar el artículo 58 bis.1 de la LOREG, es conveniente conocer cuál es la regulación de la información relativa a la ideología en el RGPD y en la LOPDyGDD. En primer lugar debemos recordar que de acuerdo con lo establecido en el artículo 2 de la LOPDyGDD, lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la Ley Orgánica 3/2018 «se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». En el apartado tercero del artículo 2 se establece que los tramitemos a los que no sea directamente aplicable el RGPD por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, «se regirán por lo dis-

---

[134] *Ibidem*.

[135] Recurso de Inconstitucionalidad contra el artículo 58 bis.1 de la LOREG.

[136] Con posterioridad a la elaboración de este trabajo, durante el proceso de evaluación, el Tribunal Constitucional ha declarado contrario a la Constitución y nulo el apartado 1 del artículo 58 bis de la LOREG en su sentencia 76/2019, de 22 de mayo.

puesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica». En esta situación se encuentran los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general.

El artículo 9 del RGPD regula el tratamiento de categorías especiales de datos personales, lo que antes denominábamos datos sensibles 137, y establece como regla general la prohibición del tratamiento de datos personales que revelen las opiniones políticas, salvo que el interesado haya dado su consentimiento explícito para uno o varios fines y siempre que el Derecho de la Unión o él estatal permitan levantar esta prohibición (art. 9.2.a) o cuando el tratamiento sea «necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado» (art. 9.2.g del RGPD). Así pues, en el RGPD, solamente con el consentimiento explícito del interesado o por razones de interés general que deberá respetar el principio de finalidad y el contenido esencial del derecho a la protección de datos personales y cuando se adopten las garantías adecuadas para proteger los derechos del interesado podrá justificarse el tratamiento de la ideología política 138. El Considerando 56 del Reglamento se refiere expresamente a la posibilidad de tratar información relativa a la ideología e indica que «si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tra-

---

[137] Estamos ante una categoría de datos personales que se refieren a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana. Por ello, las posibles agresiones a la libertad, a la intimidad, las posibilidades de ser discriminado o cualquier otra contra el ejercicio de los derechos fundamentales de las personas, se van a ver agravadas cuando los datos tratados pertenezcan a la categoría de los denominados «sensibles». La particular naturaleza de estos datos personales, por lo íntimo de las informaciones a las que hacen referencia, así como por lo particularmente graves que pueden ser las consecuencias de su utilización fraudulenta para las personas a las que se refieren, ha propiciado que en todas las regulaciones, tanto nacionales como internacionales, hayan gozado de una especial posición traducida en un reforzamiento de las medidas adoptadas para su garantía y protección. (*Vid.* Garriga Domínguez, A., *Tratamiento de datos personales y derechos fundamentales,* segunda edición, Dykinson, Madrid, 2009).

[138] La letra d) del artículo 9.2 permite también el tratamiento de estos datos «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».

tamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas».

La LOPDyGDD establece en su artículo 9 que «a los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología». No obstante, si será posible el tratamiento «de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda». En el apartado segundo del artículo 9 se establece que «los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad». Este artículo regula de forma muy restrictiva el tratamiento de los datos personales que revelen ideológica, ya que la norma española no va a permitir el tratamiento de esta categoría de datos cuya base jurídica sea el consentimiento del interesado por lo que habrá de aplicarse la excepción al régimen general contemplada en el apartado segundo de la Ley.

Por otra parte, la elaboración de perfiles se encuentra regulada en el artículo 22 del RGPD y su definición legal viene recogida en el artículo 4 del RGPD como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física». Son tres, los elementos del concepto legal: el tratamiento de los datos debe ser automatizado, debe realizarse sobre datos personales y, su finalidad, ha de ser la evaluación de algún aspecto personal de un individuo[139]. El rasgo más importante de este concepto es el de su finalidad, pues se trata de un tratamiento automatizado de datos personales cuyo objetivo es hacer una evaluación de la personalidad normalmente para hacer predicciones o inferir alguna cualidad sobre esta persona. Obviamente, al tratarse de un tratamiento de datos personales habrán de respetarse por el responsable del tratamiento todos los principios relativos al tratamiento del artículo 5 del RGPD (y del artículo 4 de la LOPDyGDD) y realizarse al amparo de alguna de las bases jurídicas para el tratamiento según lo dispuesto en el artículo 6. Igualmente habrán de respetarse los derechos de los interesados y las disposiciones que regulan las obligaciones del responsable del tratamiento sobre transparencia, seguridad y confidencialidad de la información, responsabilidad proactiva y evaluación de riesgo, privacidad desde el diseño y por defecto, etc.

---

[139] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, del Grupo de Trabajo del artículo 29, cit., p. 7.

El artículo 22 del Reglamento garantiza el derecho del interesado «a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar». No estamos ante un derecho absoluto, ya que no se aplicará este derecho cuando la decisión sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, cuando esté autorizada por el Derecho de la Unión o de los Estados miembros y establezcan asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o cuando se base en el consentimiento explícito del interesado. Incluso cuando la elaboración de perfiles se base categorías especiales de datos podrá realizarse en aquellos casos en los que se apliquen las excepciones previstas en el apartado 2, letra a) o g) del artículo 9 y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado (art. 22.4).

Los antecedentes del artículo 22 los encontramos en el artículo 15 de la Directiva 95/46/CE, que regulaba las decisiones automatizadas y en la Recomendación (2010)13 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles[140]. En esta Recomendación se destacan los peligros que la falta de transparencia en los procesos de creación de perfiles y en su posterior aplicación, los cuales podrán afectar al control de la propia identidad de la persona interesada y sus efectos serán especialmente graves cuando se realicen correlaciones utilizando datos sensibles, lo que supondrá «exponer a las personas a riesgos particularmente elevados de discriminación y de atentados contra sus derechos personales y su dignidad».

En relación con el artículo 58 bis.1 de la LOREG[141], lo primero que hay que señalar es se trata de una excepción a la prohibición gene-

---

[140] Recomendación CM/Rec(2010)13, de 23 de noviembre de 2010, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre la protección de las personas con respecto al tratamiento automático de datos de carácter personal en el contexto de perfiles.

[141] «Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.

1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

ral contenida en los artículos 9.1 del RGPD y de la Ley Orgánica 3/2018, ya que este precepto permite «la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales». La recogida de las opiniones sobre ideología, que constituye un tratamiento de datos personales de acuerdo con la definición del artículo 4 del RGPD, solo se considerará amparada en el interés público cuando se adopten las garantías adecuadas. Sin embargo, ni este ni ningún otro precepto de la LOREG o de la LOPDyGDD establece cuáles serán las garantías que se aplicarán a dicho tratamiento. La LOPDyGDD y el RGPD regulan los límites, requisitos, obligaciones y derechos de las personas concernidas para cualquier tratamiento de datos personales en su ámbito de aplicación, pero nada se dice sobre este en particular. Ha sido la Agencia Española de Protección de Datos quien ha determinado los requisitos que han de cumplir los tratamientos de datos personales regulados en el artículo 58 bis de la LOREG en su Circular 1/2019, de 7 de marzo[142] y que suponen la concreción, de acuerdo con lo establecido en la ley y en reglamento europeo, de los principios, obligaciones y derechos de los afectados en este supuesto concreto. Previamente, el 19 de diciembre de 2018, el Gabinete Jurídico de la Agencia había emitido un Informe[143] en el que entendía que el artículo 58 bis de la LOREG debía ser objeto de una interpretación restrictiva al tratarse de una excepción al tratamiento de las categorías especiales de datos personales basado en el interés público del artículo 9.2 g) del RGPD. Además el interés público actuaría como fundamento, pero también como límite, y su aplicación debe interpretarse siempre «en el sentido más favorable a la consecución de dicho interés público, por lo que en ningún caso podrá amparar tratamientos, como el *microtargeting*, que puedan ser contrarios a los principios de transparencia y libre participación que caracterizan a un sistema democrático»[144]. Así mismo, la Agencia entiende que esta interpretación restrictiva es necesaria para que las disposiciones del artículo 58 bis sean interpretadas conforme a lo establecido en la Constitución española de modo que no conculquen los derechos fundamentales a la protección de datos personales, a la libertad ideológica, la libertad de

---

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

[142] Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

[143] Informe sobre el tratamiento de datos relativos a opiniones políticas por los partidos políticos al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (N/REF: 210070/2018).

[144] Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos.

expresión e información o el derecho a la participación política[145]; pues, como he explicado, debido a su carácter instrumental, la violación del derecho fundamental a la protección de datos personales puede llevar aparejada la conculcación de otras libertades fundamentales habida cuenta de la naturaleza de los datos o de la finalidad perseguida por el tratamiento[146].

Por su parte y como ya he mencionado, el Defensor del Pueblo ha interpuesto Recurso de Inconstitucionalidad contra el artículo 58 bis.1 de la LOREG al entender que vulnera los artículos 9.3, 16, 18.4, 23.1 y 53.1 de la Constitución[147]. Entre otros motivos, para el Defensor del Pueblo, en este precepto, al no establecerse las garantías adecuadas del tratamiento de los datos ideológicos, ni precisar el interés público esencial que ampararía dicho tratamiento o el concepto de «actividades electorales», el legislador habría abdicado de *«su deber de regular concreta y pormenorizadamente las restricciones al derecho fundamental que se derivan de la autorización concedida a los partidos políticos para recopilar datos personales relativos a opiniones políticas.»*[148]

Resulta claro que las disposiciones previstas en el artículo 58 bis.1 de la LOREG constituyen un límite al derecho fundamental a la protección de datos personales y si bien podrían resultar contrarias también a los derechos garantizados en los artículos 16, 20 y 23 de la Constitución, por la naturaleza de este trabajo me centraré principalmente en el derecho del artículo 18.4 CE. La cuestión está en determinar si estamos ante una limitación que se ajusta a los cánones de constitucionalidad establecidos por nuestro Tribunal Constitucional y a los requisitos que el TEDH ha señalado para considerar la legitimidad de una injerencia o de una medida limitativa de los derechos recogidos en el artículo 8 del Convenio Europeo[149]. Como cualquier derecho fundamental, el derecho a la protección de datos personales no es un

---

[145] *Ibidem*.

[146] A modo de ejemplo puede recordarse el caso resuelto por el Tribunal Constitucional en el que el uso ilícito del dato relativo a la afiliación sindical de varios trabajadores supuso la conculcación del derecho a la protección de los datos personales y de la libertad sindical (sentencias 11/1998, de 13 de enero; 33/1998, de 11 de febrero; 35/1998, de 11 de febrero; 45/1998 de 24 de febrero; 104/1998, de 18 de mayo; 198/1998, de 13 de octubre o 44/1999, 22 de marzo; entre otras).

[147] EL Recurso ha sido admitido a trámite por el Tribunal Constitucional el 12 de marzo de 2019.

[148] P. 4 del Recurso de Inconstitucionalidad.

[149] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950. El artículo 8 del Convenio europeo de derechos humanos (el derecho a la vida privada entre el que se encontraría el derecho a la protección de datos de carácter personal) ha de interpretarse a la luz del Convenio específico sobre esta materia, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 y ratificado por España el 27 de enero de 1984. Actualmente se conoce como Convenio 108+, tras su actualización en junio de 2018, para adaptarse a la

derecho absoluto e incondicionado o carente de limitaciones, sino que puede y debe, en determinadas ocasiones, ceder ante otros valores y bienes constitucionales. Esta libertad, al igual que cualquier otro derecho fundamental, puede sufrir limitaciones, bien porque estas restricciones vengan establecidas en la Constitución directamente, bien porque deriven de ésta de manera indirecta o mediata, justificándose «por la necesidad de proteger o preservar no solo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos»[150]. Cualquier derecho fundamental «es susceptible de ser ponderado respecto de la posibilidad de hacer excepciones a dicho principio, incluyendo, desde luego, el derecho fundamental previsto en el artículo 18.4 CE en los términos y con la amplitud y autonomía que le ha sido reconocido por este Tribunal en la STC 292/2000, de 30 de noviembre, en sus fundamentos jurídicos 5 y 6»[151]. Ahora bien, los límites del derecho a la protección de datos para garantizar otros derechos y valores constitucionales han de respetar su contenido esencial. En este sentido, en su sentencia 17/2013, de 31 de enero, en la que, reiterando su fundamentación de la sentencia 292/2000, de 30 de noviembre, el Tribunal Constitucional recordaba que:

> «Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, solo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga.»

---

nueva realidad tecnológica. (https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1). Consultado e 2 de marzo de 2019.

Esta interpretación extensiva y concordante del artículo 8 del Convenio de 1950 con el Convenio de 1981 fue destacada, entre otras, en la SSTEDH Amann contra Suiza, de 16 de febrero de 2000 (TEDH 2000\87) y Rotaru contra Rumania, de 4 de mayo de 2000 (TEDH 2000\130).

[150] STC 11/1981, de 8 de abril (RTC 1981/11).

[151] STC 114/2006, de 5 de abril (RTC 2006\114).

No voy a analizar si la el tratamiento de los datos personales relativos a las opiniones políticas incumple el principio de reserva de ley respetando en todo caso los límites que se establezcan el contenido esencial de derecho fundamental[152] o si dichas garantías (las que formarían parte del haz de facultades que configuran el derecho a la protección de datos) se entenderían referidas a las establecidas en el RGPD y en la LOPDyGDD por aplicación del artículo 2 de esta última, sino que me limitaré a estudiar uno de los aspectos esenciales en la limitación del derecho garantizado por el artículo 18.4 de nuestro texto constitucional: la exigencia de proporcionalidad de la medida limitativa del derecho fundamental. En palabras del Tribunal Constitucional, el principio de proporcionalidad exige la necesidad de la limitación del derecho fundamental y que se valore «tanto la gravedad de la intromisión como su idoneidad e imprescindibilidad para asegurar la defensa del interés público (juicio de proporcionalidad)»[153]. Pero, además, el principio de proporcionalidad «no constituye en nuestro ordenamiento constitucional un canon de constitucionalidad autónomo cuya alegación pueda producirse de forma aislada respecto de otros preceptos constitucionales»[154].

---

[152] Si bien debo mencionar la doctrina del Tribunal a este respecto tal y como se recoge en el Fundamento jurídico 10 del la STC 292/2000, de 30 de noviembre, que declaró la inconstitucionalidad de varios preceptos de nuestra anterior LOPD:

«Tanto en la STC 254/1993 con carácter general como en la STC 143/1994, de 9 de mayo, F. 7, este Tribunal ha declarado que un régimen normativo que autorizase la recogida de datos personales, incluso con fines legítimos, vulneraría el derecho a la intimidad si no incluyese garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático, al igual que lo harían las intromisiones directas en el contenido nuclear de ésta.

Por tanto, las facultades legalmente atribuidas a los sujetos concernidos y las consiguientes posibilidades de actuación de éstos son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos. Asimismo, esas facultades o posibilidades de actuación son absolutamente necesarias para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos. De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (RTC 1981, 11) (F. 8), «se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección».

De este modo, la LOPD puede ser contraria a la Constitución por vulnerar el derecho fundamental a la protección de datos (art. 18.4 CE), por haber regulado el ejercicio del haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal prescindiendo de las precisiones y garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula (art. 53.1 CE).»

[153] STC 49/1999, de 5 de abril (RTC 1999\49).

[154] STC 161/1997 de 2 de octubre (RTC 1997\161). Asimismo STC 55/1996, de 28 marzo (RTC 1996\55).

De manera muy pormenorizada ha ido estableciendo el TEDH los requisitos para limitar el derecho a la protección de datos personales, que resumo a continuación. Previamente, he de señalar que si bien el artículo 8 del Convenio de 1950 prohíbe las injerencias injustificadas en la vida privada, también impone a los poderes públicos la adopción de una serie de medidas que garanticen suficientemente este derecho. En virtud de esa obligación positiva va a corresponder a los Estados adoptar todas las medidas razonables y adecuadas para proteger los derechos del artículo 8 del Convenio[155]. Si lo que se establece, como en el caso que nos ocupa, es un límite al derecho a la protección de datos personales, el Tribunal de Estrasburgo, para considerar que la injerencia constituye una medida justificada en una sociedad democrática, exigirá que tal medida limitativa esté prevista por la ley. Este primer requisito exige que la injerencia tenga una base en el Derecho interno, «pero la observancia de éste no es suficiente: la Ley enjuiciada debe ser accesible al interesado, que además, debe poder prever las consecuencias para él»[156]. Es decir, este requisito exige no solo que la medida tenga una base legal en el Derecho interno, sino que sea «accesible al justiciable y previsible»[157]. Una norma es previsible cuando está redactada con la suficiente precisión para permitir a toda persona –si es necesario, con el consejo profesional apropiado– regular su conducta. Este principio exige también que la medida limitativa del derecho a la protección de datos personales «cumpla los requisitos establecidos en la legislación interna para permitir la injerencia»[158].

En segundo lugar, la injerencia en la vida privada debe perseguir un fin legítimo, en concreto, los mencionados en el apartado segundo del artículo 8, esto es, la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y de la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y de las libertades de terceros. En relación con este requisito, el TEDH considera que va a corresponder a las autoridades internas, especialmente a los órganos jurisdiccionales, «interpretar y aplicar la legislación interna, incluso en esos campos donde el Convenio "incorpora" las reglas de esa ley donde las autoridades internas están,

---

[155] STEDH de 2 de diciembre de 2008, caso Caso K. U. contra Finlandia (TEDH 2008\95).

[156] Punto 50 del asunto Leander contra Suecia, STEDH de 26 de marzo de 1987 (TEDH 1987\4). En el mismo sentido el apartado 66 del asunto Malone contra el Reino Unido, STEDH de 2 de agosto de 1984 (TEDH 1984\1).

[157] STEDH de 16 de febrero de 2000 (caso Aman contra Suiza). En esta resolución consideró que la norma de Derecho suizo que permitía la interceptación de conversaciones telefónicas no era «previsible», porque no indicaba con la suficiente claridad el fin y las condiciones de ejercicio del poder discrecional de las autoridades. En el mismo sentido STEDH de 4 de junio de 2002, caso Landvreugd contra Holanda (JUR 2002\157827), entre otras.

[158] STEDH de 17 de julio de 2003, caso Perry contra el Reino Unido (TEDH 2003\46).

por la naturaleza de las cosas, particularmente calificadas para establecer las cuestiones que surgen a este respecto»[159].

Finalmente, la intromisión en los derechos del artículo 8 debe ser necesaria en una sociedad democrática para alcanzar tal fin. La noción de necesidad implica una exigencia o necesidad social imperiosa para la intromisión. El concepto de necesidad no equivale al de «indispensable», pero «tampoco tiene la flexibilidad de términos como "admisible", "normal", "útil", "razonable" u "oportuno"»[160]. Este último requisito exigirá normalmente la ponderación de los intereses en conflicto, el derecho o derechos afectados y la finalidad de la injerencia, o un juicio de proporcionalidad para determinar si no existe algún medio menos lesivo para vida privada que la medida adoptada y que constituye una injerencia. Así lo ha establecido el TEDH, entre otras, en la sentencia de 24 noviembre 1986 (caso Gillow contra el Reino Unido) en la que establece que «la noción de necesidad implica una injerencia basada en una necesidad social imperiosa y sobre todo proporcionada al fin legítimo perseguido». El principio de proporcionalidad, derivado de la consideración de que la medida limitativa de los derechos amparados por el artículo 8 del Convenio ha de ser necesaria en una sociedad democrática, implica una doble consideración, tanto de procedimiento como de fondo[161]. Primero, habrá de examinarse «la decisión material de las autoridades internas para asegurar que es compatible con el artículo 8»[162] y, en segundo lugar, se estudiará el proceso de decisión para establecer si se han tenido suficientemente en cuenta los intereses de las personas. Pues, es preciso verificar «si el proceso de toma de decisiones que llevó a la medida de la injerencia fue justo y de tal forma concedió el debido respeto a los intereses garantizados por el artículo 8 para el individuo»[163]. El principio de proporcionalidad exige, en definitiva, que «los Estados que minimicen, hasta donde sea posible, la injerencia en estos derechos, intentando encontrar soluciones alternativas y buscando en general, alcanzar los fines de la forma menos onerosa para los derechos humanos»[164]. El TEDH exige que se aplique el principio de proporcionalidad determinando, si la injerencia está justificada, es racional y es proporcionada. Se hace necesario, por tanto, buscar el imprescindible equilibrio que en las

---

[159] STEDH de 5 de diciembre de 2013, caso Skrtic contra Croacia (TEDH 2013\89).

[160] Ruiz Miguel, C., *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos,* 1994, p. 104-105.

[161] Entre otras, STEDH de 5 de diciembre de 2013, caso Skrtic contra Croacia (TEDH 2013\89).

[162] STEDH de 10 de noviembre de 2004, caso Taskin y otros contra Turquía (TEDH 2004\85).

[163] STEDH de 27 de mayo de 2004, caso Connors contra el Reino Unido (JUR 2004\158847).

[164] STEDH de 2 de octubre de 2001, caso Hatton y otros contra el Reino Unido (TEDH 2001\567).

sociedades democráticas deben tener las actuaciones de las autoridades internas restrictivas de derechos fundamentales y los propios derechos de las personas, que forman un conjunto de valores fundamentales en nuestras sociedades democráticas y de Derecho.

En el caso del artículo 58 bis.1 de la LOREG el juicio de proporcionalidad habrá de ser si cabe más riguroso ya que permite la recolección de una categoría de datos especialmente sensible susceptible de revelar la ideología política de las personas a las que se refieren. Para aplicar las reglas anteriores, debemos en primer lugar determinar cuál es la finalidad perseguida por esta norma, para valorar si es necesaria, adecuada y si no existe un medio menos lesivo para el derecho fundamental para lograrla. Por su incardinación en la Sección 5.ª sobre «Propaganda y actos de campaña electoral» del Capítulo VI de la Ley que regula el procedimiento electoral podríamos pensar que la finalidad del tratamiento de los datos sobre opiniones políticas sería la de conocer la opinión social sobre cuestiones políticas importantes que serían tenidas en cuenta para la elaboración de los programas electorales y durante los actos de campaña, así como para el diseño de la publicidad electoral. No obstante y esta es una cuestión fundamental, la finalidad de la recogida de los datos personales relativos a opiniones políticas no está explicitada en el artículo de la LOREG de forma que difícilmente podemos saber si se trata de una finalidad que quedaría amparada en un interés público esencial tal y como exige el artículo 9 del RGPD. Por su parte el Considerando 56 del RGPD, que se citaba en la enmienda 331 introducida durante la tramitación del Proyecto de Ley de Protección de Datos de Carácter Personal como justificación de la misma, considera la posibilidad de que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, cuando en el marco de actividades electorales, el funcionamiento del sistema democrático lo exigiera. Confieso que soy incapaz de imaginar ninguna situación en la que el funcionamiento del sistema democrático pueda requerir que los partidos políticos recopilen datos personales relativos a la ideología de personas concretas, fuera del supuesto de sus afiliados en los términos del artículo 9.2.d) del RGPD. No olvidemos que un dato personal es aquella información relativa a una persona física identificada o identificable. Para cumplir la función esencial que los partidos políticos desempeñan en un Estado democrático en período electoral y que, citando una vez más la sentencia 136/1999 de nuestro Tribunal Constitucional, formaría parte del inescindible contenido del principio de representación política, que conecta los derechos de participación en los asuntos públicos y de acceso a los cargos públicos y que se concreta «en la posibilidad constitucionalmente protegida de ofrecer a los ciudadanos, sin interferencias o intromisiones de los poderes públicos, los análisis de la realidad social, económica o política y las propuestas para transformarla que consideren oportunas», no parece necesario identificar a personas determinadas por su ideología, convicciones morales o inquietudes

políticas. El principio de representación política garantiza valores y principios constitucionales, que sí pudieran constituir el un interés público esencial del artículo 9.2.g) del RGPD y del artículo 9.2 de la LOPDyGDD en relación con el interés público al que se refiere el artículo 58 bis.1 de la LOREG. Y, a través de la difusión de programas o mensajes electorales, «las personas que participan como actores en la actividad pública, y a los partidos y grupos en los que se integran tienen «la posibilidad de contribuir a la formación y expresión de la opinión pública libre, poniendo a disposición de los ciudadanos en general y de los electores en particular una pluralidad de opciones políticas para que puedan formar sus propias opiniones políticas y, en el momento electoral, para que puedan elegir libremente los programas que estimen más adecuados»[165], contribuyendo a la realización de los principios de la legitimidad democrática del sistema político, el pluralismo político y la formación de la opinión pública libre, que son valores esenciales en una sociedad democrática.

Pero, para cumplir tan esencial función, no es necesario recabar las opiniones políticas de personas determinadas, ni identificarlas, si siquiera en mi opinión, justificaría la recolección de dichas informaciones aunque fueran posteriormente seudonimizadas[166]; informaciones sobre cuestiones políticas disociadas de las personas que las emitieron, es decir, los datos anónimos de forma que el interesado no sea identificable, o deje de serlo, cumplirían igualmente esta finalidad y si se manejaran datos estadísticos anónimos y sondeos de opinión elaborados a través de las manifestaciones que las personas y los diferentes grupos y comunidades expresan por los distintos medios a su alcance, incluidas las plataformas sociales, no resultaría afectado el derecho a la protección de datos personales, con lo que se cumpliría con las exigencias del principio de proporcionalidad. Y, protegiendo los datos personales de quienes libremente se expresan en el ámbito digital se garantiza el pluralismo de ideas y opiniones, las libertades de expresión, ideológica y el derecho de participación política y se realizaría más eficazmente el principio democrático a través de un debate no vigilado. Precisamente, por esta razón, la Circular 1/2019 de la Agencia considera desproporcionados los tratamientos de *microtargeting* o que tengan como finalidad forzar o desviar la voluntad de los electores y si se pretende la elaboración de perfiles, considera únicamente admisibles «la elaboración de perfiles generales y por categorías genéricas, pero no la realización de perfiles individuales o realizados atendiendo a categorías muy específicas, de tal manera que solo se puedan deducir patro-

---

[165] STC 136/1999.

[166] El artículo 4 del RGPD define la seudonimización como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable».

nes de conducta generales de la población de forma agregada, pero no de titulares de datos personales concretos» (art. 6).

VI. CONCLUSIONES

El fenómeno de la desinformación no es nuevo, las teorías de la conspiración, los rumores sin verificar, los bulos o las mentiras sobre hechos objetivos o sobre personas ya existían antes de Internet y del desarrollo de las plataformas sociales. Sin embargo, «la diferencia con las *fake news* de hoy es que, con las plataformas digitales que dan sostén a las «redes sociales» y permiten la masiva generación e intercambio de contenidos, la desinformación multiplica y disemina de forma exponencial en tiempo real sin espacio para la reflexión o corrección»[167]. Por otra parte, los filtros burbuja que explotan el sesgo de confirmación limita nuestra visión del mundo y consecuentemente nuestra capacidad para conocer y comprender la realidad y los puntos de vista de aquellos que por disentir de nuestra opinión son relegados por un sistema de inteligencia artificial. Estos mismos algoritmos para maximizar su eficiencia refuerzan las emociones negativas que son más productivas para incrementar el tiempo que pasamos conectados y captar nuestra atención.

Los procesos y las herramientas tecnológicos que confluyen en este fenómeno tan complejo son de difícil compresión para el usuario medio y su funcionamiento es poco transparente[168]. La propia lógica del diseño del modelo de negocio que se basa en la recogida masiva de datos personales para ser reelaborados en el ámbito de la realización de perfiles predictivos, que buscan condicionar el comportamiento de los individuos con diversos fines publicitarios y de marketing, son mucho más eficientes si este es un proceso es opaco.

Los recientes escándalos relacionados con la influencia del fenómeno de la desinformación a través de las redes sociales han tenido como consecuencia que estos servicios adopten determinadas medidas correctoras para luchar contra las noticias falsas en sus medios[169] y que

---

[167] Gutiérrez, M., «Manual de fake news: El papel de los sesgos cognitivos», *eldiario.es* (https://www.eldiario.es/tecnologia/Manual-fake-papel-sesgos-cognitivos_0_841316711.html). Consultado el 3 de diciembre de 2018.

[168] Recientemente, la Autoridad de control francesa, la Comisión Nacional de Informática y Libertades (CNIL) ha multado a Google por violar el principio de transparencia, por facilitar información de forma incorrecta, ya que no es fácilmente accesible como exige la normativa europea, y por no obtener de forma válida el consentimiento de los usuarios de sus servicios en el ámbito de la publicidad personalizada con 50.000.000 de euros en aplicación del RGPD. https://elpais.com/economia/2019/01/21/actualidad/1548088756_370588.html (consultado el 22 de enero de 2019).

[169] *Vid.*, entre otros, «Así intentarán las redes sociales frenar los bulos ante las próximas elecciones». https://www.publico.es/politica/desinformacion-intentaran-redes-sociales-frenar-bulos-proximas-elecciones.html (consultado el 22 de marzo de 2019);

los gobiernos incluyan en sus planes de ciberseguridad los riesgos de las campañas de desinformación [170]. En el ámbito de la Unión Europea, la Comisión[171], reconociendo «que las campañas masivas de desinformación en línea con motivos políticos, particularmente a cargo de terceros países, con el objetivo específico de desacreditar y deslegitimar las elecciones constituyen amenazas crecientes» para las democracias, ha presentado una serie de medidas para garantizar las elecciones de 2019 al Parlamento Europeo. Éstas se centran en la aplicación rigurosa del RGPD y de la Directiva 2002/58/CE, que garantiza la confidencialidad de las comunicaciones electrónicas, en una serie de recomendaciones para luchar contra la desinformación en línea, en «abordar las situaciones en las que los partidos políticos o sus fundaciones asociadas se beneficien de prácticas que infrinjan las normas de protección de datos, con vistas a influir o intentar influir de forma deliberada en el resultado de las elecciones europeas» y en la aprobación de un Código de buenas prácticas en materia de desinformación[172].

Sin duda estas medidas contribuirán a combatir la desinformación durante los procesos electorales; sin embargo, en mi opinión, se trata de soluciones insuficientes. Debe exigirse que los procesos de perfilado, que afecta a las oportunidades vitales de las personas, que dependen de la categoría en la que las hayan situado y que permite condicionar su conducta a través de la seducción, como señaló Bauman, sean completamente transparentes respecto de cómo se elaboran, para qué y para quienes, tal y como exige el RGPD. Cuando cualquier decisión se adopta con base en un perfil, incluida la información a la que tendremos acceso, el principio de transparencia es imprescindible para poder conocer quién diseña esas categorías en las que se nos clasifica, quién decide sus significado y quién decide bajo qué circunstancias esas categorías serán decisivas[173]. Pues, como ha indicado el Supervisor Europeo de Protección de Datos, la correcta aplicación de las normas europeas que garantizan la protección de los datos personales y la confidencialidad de las comunicaciones electrónicas «debería ayudar a minimizar los daños causados por los intentos de manipular a los

---

[170] «Cien policías blindarán el 28-A contra bulos y ataques informáticos». https://elpais.com/politica/2019/03/14/actualidad/1552571931_168409.html (consultado el 15 de marzo de 2019).

[171] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Garantizar unas elecciones europeas libres y justas de 12 de septiembre de 2018. https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-637-F1-ES-MAIN-PART-1. PDF (consultado el 24 de octubre de 2018).

[172] Entre los firmantes del Código en octubre de 2018 estarían Google, Facebook, Twitter, Mozilla y las asociaciones empresariales que representan al sector de la publicidad. *Vid.* europa.eu/rapid/press-release_IP-19-746_es.pd (consultado el 3 de febreo de 2019).

[173] D. Lyon, *Surveillance Studies. An overview*, cit., p. 186.

grupos»[174]. No obstante, es imprescindible también la exigencia de responsabilidad a «los actores de ecosistema (digital) que se benefician de las conductas nocivas»[175], ya que la apelación a la transparencia no es suficiente.

Igualmente debería valorarse la propuesta que el Parlamento Europeo[176] ha realizado en el contexto del escándalo Cambridge Analytica, considerando que debería «prohibirse la elaboración de perfiles para fines políticos y electorales, y la elaboración de perfiles sobre la base de comportamientos en línea que puedan revelar preferencias políticas». Asimismo, considera que debería prohibirse la elaboración de perfiles sobre la base de otros datos para fines políticos o electorales y «pide a los partidos políticos y a otros actores que participen en las elecciones que se abstengan de utilizar perfiles para fines políticos y electorales» y que sean transparentes «en lo que respecta a su utilización de las plataformas y los datos en línea».

---

[174] Resumen del Dictamen del SEPD sobre la manipulación en línea y los datos personales. DOUE de 4 de julio de 2018.

[175] *Ibidem*.

[176] 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.