Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales

Juan Manuel López Ulla

Profesor Titular de Derecho Constitucional

Universidad de Cádiz
España

ORCID 0000-0001-6595-6183

RECIBIDO: 28 de enero de 2024

ACEPTADO: 20 de marzo de 2024

RESUMEN: En aras de una mayor transparencia en el tratamiento de los datos personales, este artículo plantea la posibilidad de modificar el art. 22 del Reglamento General de Protección de datos de la Unión Europea para que la prohibición general que este precepto ordena no se ciña a la elaboración de perfiles que pudieran producir efectos *ad personam*, sino también a otra clase de prácticas que puedan afectar a toda la comunidad política, como las que tratan de manipular a segmentos enteros de la población con el objetivo de interferir en los procesos democráticos. Al efecto, recordamos que el derecho a la protección de datos debe estar dotado de garantías adecuadas y que los instrumentos de defensa que el ordenamiento jurídico contempla no están pensados para este entorno en el que las amenazas tienen otro alcance. En este nuevo marco jurídico, también sería recomendable conceder una nueva textura constitucional al derecho a la protección de datos personales y al derecho de acceso a la información pública. Estas conclusiones se apoyan en los documentos más relevantes aprobados en el seno de la UE en los últimos tres años, en la jurisprudencia del TJUE y del TEDH y en las aportaciones más recientes de la doctrina, que advierten la necesidad de reglas más claras y precisas que permitan compatibilizar el desarrollo de la tecnología con los derechos de las personas.

PALABRAS CLAVE: Protección de datos personales, perfilado ideológico, democracia, elecciones, manipulación política.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

CONTENIDOS: 1.- Garantías adecuadas frente a los sistemas inteligentes que automatizan el análisis de la información. 2.- Sobre la conveniencia de conceder una nueva textura constitucional a la protección de datos personales y al derecho de acceso a la información pública. 3.- En torno a la posibilidad de que los partidos puedan recabar datos que revelen la opinión política de los electores. 4.- Sobre el riesgo cierto de que las nuevas tecnologías puedan interferir en los procesos de deliberación democrática. 5.- Algunas medidas que pudieran reducir el riesgo de manipulación política a partir del tratamiento inteligente de los datos personales. 6.- Recapitulación. - Bibliografía.

Appropriate safeguards to protect democracy against the fraudulent use of personal data

ABSTRACT: In the interest of greater transparency in the processing of personal data, this article raises the possibility of amending art. 22 of the GDPR so that the general prohibition established by this provision should not only cover the creation of profiles that could produce ad personam effects, but also other types of practices that could affect the entire political community, such as those that aim to manipulate large segments of the population with the intention of interfering in democratic processes. In this regard, it is important to remember that the right to data protection must be effectively protected with adequate guarantees. It is therefore necessary to check whether the legal system has the appropriate tools to deal with the potential threats associated with new technologies. In this new legal framework, it might be useful to give a new constitutional texture to the right to personal data protection and also to the right to access public information. These conclusions are based on the most relevant documents approved within the EU in the last three years, on the case law of the CJEU and the ECtHR, and on the most recent contributions published on this topic, which highlight the need for clearer and more precise rules that allow the harmonious coexistence of technological development with the protection of fundamental rights.

KEYWORDS: Data protection, political profiling, democracy, elections, political manipulation.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

1.- Garantías adecuadas frente a los sistemas inteligentes que automatizan el análisis de la información

La Sentencia del Tribunal Constitucional (STC) 254/1993, de 18 de agosto, reconoció en el art. 18.4 CE "una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona frente al uso de la informática" (FJ. 6), pero empleando el concepto de "libertad informática" o *habeas data*. La primera sentencia en hablar del "derecho fundamental a la protección de datos personales" fue la STC 290/2000, de 30 de noviembre (FJ. 7). La STC 292/2000, de la misma fecha, subrayó la necesidad de establecer las garantías adecuadas "para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos" (FJ. 10). Recordando esta jurisprudencia, la STC 76/2019, de 22 de mayo, advierte que estas garantías no pueden quedar obsoletas; que para que sean adecuadas deben de corresponderse con las potenciales amenazas que la tecnología pueda generar (FJ. 6).

A los efectos de este comentario, huelga cualquier consideración sobre los riesgos que para los derechos comportan, a modo de daños colaterales, los avances de las ciencias de la informática. Si se nos permite la superficialidad de la explicación, los entornos virtuales funcionan porque existe una tecnología que permite el procesamiento de un gran volumen de datos. La capacidad, cada vez mayor, para generar información a partir de ellos, mediante algoritmos (fórmula matemática que le dice a un sistema cómo debe procesar los datos a su disposición) e inteligencia artificial[1] exige que los sistemas de garantías estén actualizados. "Sin negar las grandes ventajas que esta nueva etapa representa, la edad digital plantea también nuevas amenazas para las personas y para sus derechos, que antes no existían" (Troncoso Reigada, 2023: 240).

Los instrumentos de defensa que un ordenamiento jurídico contempla se corresponden normalmente con los tipos de amenazas latentes en cada momento de la historia, no con las que están por venir, de ahí la necesidad de establecer un marco jurídico que permita desarrollar esta nueva tecnología sin que ello repercuta negativamente en nuestras cartas de derechos. Para ello, una condición *sine qua non* ha de ser la obligación de proporcionar la información adecuada sobre los algoritmos utilizados en estos procesos, advierten entre otros Medina Guerrero (2022: 142-143), Jiménez-Castellanos Ballesteros (2023: 191-215), o Cotino Hueso (2023, pp. 17-63). De lo contrario, sería difícil avanzar en transparencia y rendición de

[1] El art. 3.1 del *Reglamento de IA* define de la siguiente manera el concepto «sistema de IA»: se trata de "un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales" (Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

cuentas. Además del *Reglamento General de Protección de Datos* de la UE (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, algunos de los textos más recientes que han expresado esta preocupación sobre la necesidad de salvaguardar los derechos de las personas frente a la capacidad presente y futura de estos sistemas inteligentes son los siguientes (la relación no atiende al carácter normativo o no de los mismos):

El *Convenio 108 modernizado* o *Convenio 108+*, aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, actualizando el Convenio de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[2] - que aún sigue en fase de ratificación -, se justifica por la necesidad de hacer frente a los retos derivados de la utilización de las nuevas tecnologías de la información y la comunicación, de la globalización de las operaciones de tratamiento y del aumento del flujo de datos personales[3].

La *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* (2023/C 23/01), adoptada el 15 de diciembre de 2022 por el Parlamento Europeo, el Consejo y la Comisión, se aprueba con la intención de orientar el enfoque de la UE con respecto a la transformación digital a partir del respeto a los valores y derechos consagrados en su Carta de Derechos Fundamentales[4].

Con este mismo enfoque, el *Reglamento de IA*, de 13 de marzo de 2024 (cit.), se aprueba con el objetivo de "mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial («sistemas de IA») en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (la «Carta»), en particular la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación" (primer Considerando).

Otros textos de la UE que han expresado su preocupación por la protección de los derechos fundamentales frente a las nuevas tecnologías son: el *Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021 por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE)*

[2] Instrumento de ratificación publicado en el *Boletín Oficial del Estado* núm. 274, de 15 de noviembre de 1985.

[3] El Convenio 108+ es accesible a través del siguiente enlace: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[4] *Diario Oficial de la Unión Europea* núm. 66, de 23 de enero de 2023, p. 1.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

2015/2240[5]; la *Resolución del Parlamento Europeo, de 20 de enero de 2021, sobre inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho internacional en la medida en que la UE se ve afectada en los ámbitos de los usos civil y militar, así como de la autoridad del Estado fuera del ámbito de la justicia penal* [2020/2013(INI)]; la *Resolución, de 6 de octubre de 2021, sobre la utilización de la Inteligencia Artificial en el ámbito penal por las autoridades policiales y judiciales en asuntos penales* [2020/2016(INI)]; y las siguientes Comunicaciones de la Comisión Europea: *Inteligencia artificial para Europa* [COM(2018) 237 final, de 25 de abril de 2018]; *Plan coordinado sobre la inteligencia artificial* [COM(2018) 795 final, de 7 de diciembre de 2018]; *Generar confianza en la inteligencia artificial centrada en el ser humano* [COM(2019) 168 final, de 8 de abril de 2019]; y el *Libro Blanco sobre inteligencia artificial– un enfoque europeo orientado a la excelencia y a la confianza* [COM(2020) 65 final, de 19 de febrero de 2020].

Fuera del marco de la UE, la *Carta Iberoamericana de Principios y Derechos en los Entornos Digitales*, adoptada en el marco de la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada en Santo Domingo (República Dominicana) en marzo de 2023, también deja constancia de esta preocupación, pues comienza de la siguiente manera: "La digitalización conlleva una profunda transformación que impacta en todos los aspectos de la vida de las personas y presenta enormes desafíos, que deben abordarse garantizando el ejercicio de los derechos, el cumplimiento de los deberes y el desarrollo de sociedades digitales inclusivas, justas, seguras, resilientes y sostenibles"[6].

A nivel interno, y con esta misma intención de ofrecer "un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital", y de identificar "los principios que han de guiar la acción pública en los ámbitos más directamente afectados por la digitalización", el Gobierno de España adoptó, el 14 de julio de 2021, un texto programático - sin fuerza jurídica - que trata de establecer unas directrices para la salvaguarda de los derechos fundamentales en el entorno digital, la Carta de Derechos Digitales. Sus "Consideraciones Previas" advierten cómo "el intenso progreso de la investigación científica, las invenciones y las tecnologías digitales o basadas en lo digital plantean la necesidad de asegurar que el marco normativo garanti[ce] la protección de los derechos individuales y colectivos de las personas, [y] los valores constitucionales que constituyen el único cimiento posible de la convivencia". No se trata "de crear nuevos derechos fundamentales [advierte el texto] sino de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros".

[5] El citado Reglamento (UE) está publicado en el *Diario Oficial de la Unión Europea*, núm. 166, de 11 de mayo de 2021.

[6] La *Carta Iberoamericana de Principos y Derechos en Entornos Digitales* es accesible a través del siguiente enlace: https://www.segib.org/?document=carta-iberoamericana-de-principios-y-derechos-en-entornos-digitales

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

En esta misma dirección, el artículo 23 de la *Ley 15/2022, de 12 de julio, integral de igualdad de trato y de no discriminación* ordena en su párrafo primero que las Administraciones Públicas favorezcan "la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente"; y su párrafo tercero, atendiendo a la *Recomendación sobre la ética de la inteligencia artificial* aprobada por la UNESCO el 23 de noviembre de 2021[7], ordena que las administraciones públicas y las empresas promuevan "el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido". Por lo que a esta última referencia se refiere, el Preámbulo de la Declaración Europea sobre los Derechos y Principios Digitales recuerda que "el Parlamento ha pedido en varias ocasiones el establecimiento de principios éticos que guíen el enfoque de la UE con respecto a la transformación digital, y que se garantice el pleno respeto de derechos fundamentales como la protección de datos, el derecho a la privacidad, la ausencia de discriminación, la igualdad de género, y de principios como la protección de los consumidores, la neutralidad tecnológica y de la red, la fiabilidad y la inclusividad" (parágrafo 4)[8].

La preocupación "por el profundo influjo que las tecnologías de la información y la comunicación tienen sobre la vida humana" (Revenga Sánchez, 2023: 37) resulta evidente. El denominador común que se deriva de los textos hasta aquí citados es el interés por establecer un marco jurídico para que el desarrollo de toda esta tecnología no repercuta negativamente en los derechos de las personas, sino que "quede dentro de lo constitucionalmente admisible" (Sánchez Barrilao, 2016: 255). Se trata, una vez más, de afrontar la difícil tensión entre los derechos y el mercado, como advierte con toda claridad la Exposición de Motivos del *Reglamento de IA* (cit.).

En la construcción de este marco jurídico, el Tribunal de Justicia de la Unión Europea (TJUE) jugará un papel importante en la interpretación y aplicación de la normativa europea de protección del derecho fundamental a la protección de datos, y no solo en el territorio de la Unión. Rallo Lombarte (2017: 584) así lo advierte tras un detenido análisis de tres sentencias señeras que "marcan un hito en la evolución de la protección de los datos personales frente a la globalización tecnológica por su impacto mundial, esto es por la expansión de los estándares europeos de protección al resto de latitudes del planeta" [*Caso Digital Rights* (Directiva conservación de

[7] *Recomendación sobre la ética de la inteligencia artificial*, adoptada el 23 de noviembre de 2021 por la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). Accesible a través del enlace: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

[8] Documento 2023/C 23/01, *Diario Oficial de la Unión Europea* núm. 66, de 23 de enero de 2023, p. 1.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

datos[9]), *Caso Google* (derecho al olvido)[10] y *Caso Facebook* (Safe Harbour)[11]]. En todas ellas se advierten los enormes riesgos potenciales para la privacidad del individuo que deriva del uso de servicios y dispositivos tecnológicos.

2.- Sobre la conveniencia de conceder una nueva textura constitucional a la a la protección de datos personales y al derecho de acceso a la información pública

"Las nuevas formas de comunicación y socialización asociadas al uso (y al abuso de las tecnologías de la información y la comunicación plantean desafíos inéditos que convierten las regulaciones constitucionales en estipulaciones «declinantes» cuando no vacías o privadas de sentido, como consecuencia de una «nueva normalidad» que a menudo las sobrepasa y desmiente" (Revenga Sánchez, 2023: 41). Un primer paso en esta dirección quizá pudiera ser que la Constitución expresamente se refiriera al derecho a la protección de datos de carácter personal. Es cierto que el TC ya lo ha reconocido en el art. 18.4 CE, pero, como es sabido, de la literalidad de este precepto lo que se deriva no es un derecho sino un mandato al legislador para que proteja el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos de los ciudadanos frente al uso de la informática.

Dado que "internet (…) se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva", una actualización de la Constitución que elevara "a rango constitucional una nueva generación de derechos digitales", que es lo que reclama el apartado IV del Preámbulo de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, no podría, a nuestro juicio, dejar de invocar por su nombre el derecho a la protección de datos personales. La trascendencia que este derecho ha adquirido en este entorno justificaría esta nueva textura constitucional que le concedería este reconocimiento expreso, como entre otros ha reclamado Bilbao Ubillos (2019: 98).

Una hipotética reforma constitucional en torno a este derecho pudiera ser también aprovechada para zanjar el debate abierto entre la doctrina sobre el posible carácter fundamental del derecho de acceso a la información, naturaleza que evidentemente no tiene mientras esté ubicado en el art. 105.b) CE, lo que no ha impedido que algunos autores hayan advertido la relación directa que este derecho tiene con la libertad de información. No nos estamos refiriendo al derecho que el art. 15.1 RGPD reconoce al interesado "a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la (…) información", sino al derecho que el ciudadano tiene a conocer los procesos lógicos-jurídicos que motivan la decisión que pudiera afectarle. Dicho de otra manera, si las personas pueden ser objeto de

[9] STJUE de 8 de abril de 2014 (*C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros vs. Irish Data Protection Comissioner*)

[10] STJUE de 13 de mayo de 2014 (C-131/12, Caso Google vs. AEPD)

[11] STJUE de 6 de octubre de 2015 (Caso 362/14 Maximillian Schrems/Data Protection Commissioner).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

una decisión automatizada o de un perfilado a partir de sus datos personales, el acceso a los algoritmos que hayan conducido a tal resolución y/o a la información y los métodos empleado a tales efectos resultará imprescindible para garantizar la transparencia de tales procesos. Como Revenga Sánchez advierte, "el algoritmo no puede tener la última palabra cuando lo que está en juego son los derechos fundamentales de los ciudadanos" (2023, 44).

Entre los autores que se han manifestado al respecto, Cotino Hueso (2017: 279) no tiene dudas de que el derecho de acceso a la información pública se ha conformado internacionalmente como un derecho fundamental, aunque tal reconocimiento "no se haya consolidado" en España. López Aguilar se pronuncia en el mismo sentido, recordando que este derecho ya está contemplado en el art. 42 de la Carta de Derechos Fundamentales de la UE (2023:29)[12]. Fernández Ramos y Pérez Monguío (2017: 15) no se pronuncian en concreto sobre ese aspecto, pero advierten la relevancia capital de este derecho "por su innegable vinculación con el mismísimo principio democrático". Ruiz-Rico Ruiz (2021:71-72) destaca que, si bien "la transparencia adquiere la condición de valor constitucional, por su evidente conexión con otros principios y valores del mismo rango", esto no es suficiente para concebirlo como "un derecho público subjetivo, dotado de las características de inmediatez y aplicabilidad directa". Dicho esto, admite la conexión evidente de este derecho con la libertad consagrada en el art. 20.1.d) CE, y la importancia de la transparencia para el sistema democrático, en la medida en que el acceso a la información pública representa una garantía instrumental del derecho de participación (art. 23 CE). Carrillo (2015: 269) no cree que el derecho de acceso a la información pública haya sido configurado constitucionalmente como un derecho fundamental sino más bien como un "principio jurídico". Rey Martínez (2014: 12) recuerda que, si bien "el legislador no puede crear derechos fundamentales, (…) sí puede reconocerlos a partir de su relación con otros derechos fundamentales expresos", advirtiendo la relación de este derecho con los derechos a recibir información veraz (art. 20.1.d) y a participar directamente en los asuntos públicos (art. 23.1). Y Villaverde Menéndez (2019: 168 y 171) reconoce que la transparencia "se erige en un valor constitucional" como "expresión e instrumento necesario del ejercicio de los derechos fundamentales a recibir información y a participar en los asuntos públicos, y como medio para la más óptima realización de los principios del Estado democrático y de derecho", pero critica "la invención de un derecho fundamental a la transparencia o de un principio constitucional a la transparencia que a su juicio no existen en el caso de la Constitución española".

Como se habrá apreciado, más allá de la posición de estos autores sobre si el derecho de acceso a la información es o no un derecho fundamental, todos ellos coinciden en subrayar su conexión con la libertad de información reconocida en el

[12] Art. 42 de la Carta de Derechos Fundamentales de la Unión Europea: reconoce el derecho de "todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

art. 20.1 d) CE. Sin embargo, la sentencia del Tribunal Supremo (STS) 140/2023, de 7 de febrero, no lo ha entendido así, pues en ella se sostiene que el acceso a la información pública [art. 105.b) CE] ni es un derecho fundamental ni guarda la más mínima relación con la libertad de información [art. 20.1.d) CE].

Efectivamente, el Fundamento de Derecho 4 de esta sentencia reconoce que el acceso a la información pública es al mismo tiempo "un principio objetivo rector de la actuación de las Administraciones Públicas (art. 103.1 CE), que se deriva de las exigencias de democracia y transparencia", y "un derecho subjetivo de las personas, ejercitable frente a las Administraciones Públicas, según declara la STC 164/2021, de 4 de octubre". Pero de lo anterior no se deriva, advierte el TS, que se trate un derecho fundamental o que el art. 20.1.d) pueda prestar cobertura a quien solicite el acceso a unos archivos o registros públicos. Aunque se trate de un derecho "acorde con los principios inherentes al Estado democrático (en cuanto el acceso a los archivos y registros públicos implica una potestad de participación del ciudadano y facilita el ejercicio de la crítica del poder), y al Estado de Derecho (en cuanto dicho acceso constituye un procedimiento indirecto de fiscalizar la sumisión de la Administración a la ley y de permitir con más eficacia el control de su actuación por la jurisdicción contencioso-administrativa)", para el TS "este derecho se sitúa fuera del perímetro de protección que establece el art. 53.2 CE" (*Ibidem*, Fundamento de Derecho 5).

Esta posición del TS negando la conexión del derecho de acceso a la información pública con el derecho fundamental a la libertad de información no solo es contraria a la postura mayoritaria de la doctrina científica sino también a la jurisprudencia del TEDH, que en varias de sus sentencias ha ubicado el derecho de acceso en el art. 10.1 CEDH (libertad de expresión): en *Youth Initiative for Human Rights c. Serbia*, n. 48135/2006, de 25 de junio de 2013, la demanda fue estimada porque se consideró que la decisión de las autoridades competentes negando el acceso a la información pública solicitada había supuesto una injerencia en el derecho a la libertad de expresión de la demandante; *Magyar Helsinki Bizottság c. Hungría* (Gran Sala), n. 18030/11, de 8 de noviembre de 2016, también ubicó este derecho en el marco del derecho a la libertad de expresión; en *Szurovecz c. Hungría*, n. 15428/16, de 8 de octubre de 2019, el TEDH consideró, igualmente, que la libertad de expresión reconocida en el art. 10.1 CEDH comprendía el derecho de acceso a la información de interés público. No parece, pues, que el TS haya tomado en consideración esta jurisprudencia al dictar la sentencia referida en nuestro párrafo anterior. Porque resulta evidente que "en algunos casos, el derecho de acceso a la información pública es el instrumento necesario para poder ejercer el derecho fundamental a la libertad de información" (Blanes Climent, 2023), parece razonable que el procedimiento especial para la protección de los derechos fundamentales previsto en la Ley 29/1998, Reguladora de la Jurisdicción Contencioso-Administrativa, pudiera ser invocado cuando quedara patente su relación con la libertad de información, tal y como ha reconocido el TEDH. Esta falta de sintonía entre la doctrina del TS y la jurisprudencia de este Tribunal, que contraviene el mandato del

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

art. 10.2 CE, quizá pudiera ser interpretada como una señal sobre la conveniencia de modificar la Constitución en este sentido.

A partir de aquí, el debate en torno a si la Constitución debe reconocer nuevos derechos para responder mejor a las exigencias de la persona en la edad digital está servido. La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales sí lo hace, proclamando, entre otros, los derechos de acceso a internet, de neutralidad de la Red, a la identidad en el entorno digital, al olvido, a la desconexión digital en el marco del derecho a la intimidad o el de rectificación en internet (López Ulla, 2021: 4007). Que a estos se les deba conceder la textura constitucional que para aquellos otros hemos abogado no está tan claro, pero por razones de espacio no podemos ahora detenernos en esta cuestión. Las posturas al respecto las resume bien Troncoso Reigada (2023: 241), advirtiendo que pueden sintetizarse en dos: la de quienes, con una visión más humilde, consideran que en puridad no se trata de descubrir nuevos derechos como si fueran algo distinto a los derechos fundamentales ya reconocidos, sino de abordar el reto que supone la interpretación y aplicación de los derechos de siempre al entorno digital; y la de quienes, con un planteamiento más ambicioso, abogan por el reconocimiento de nuevos derechos fundamentales, que se encuadrarían en una nueva categoría, la de los derechos digitales, que conformarían una nueva generación de derechos.

3.- En torno a la posibilidad de que los partidos puedan recabar datos que revelen la opinión política de los electores

La STC 76/2019 declaró la inconstitucionalidad del art. 58 bis, apdo.1 de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG). Este precepto permitía que "en el marco de sus actividades electorales", los partidos políticos pudieran recopilar "datos personales relativos a las opiniones políticas de las personas" cuando el "interés público" así lo justificara y con las "garantías adecuadas"[13]. El recurrente (Defensor del Pueblo) había denunciado la posible lesión del art. 18.4 CE en conexión con el art. 53.1, en cuanto que la disposición impugnada no concretaba de manera alguna el marco que justificaba el tratamiento, la finalidad del mismo ni las garantías adecuadas a las que hacía referencia el precepto en su parte final, vulnerando de esta manera la reserva de ley que la Constitución ordena sobre el derecho a la protección de datos, y, por ende, su contenido esencial.

En defensa de la validez del precepto, la abogacía del Estado alegó que su base jurídica se encontraba en el Considerando 56 del RGPD, que dice así: "Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas". El

[13] Art. 58 bis, apdo.1 LOREG: "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".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

problema radicaba en que la disposición impugnada no concretaba en absoluto tales garantías.

Más allá de este Considerando, que no tiene valor normativo sino meramente interpretativo, la base jurídica de la recopilación de esta clase de datos políticos o ideológicos se encuentra en el art. 9.2 RGPD, que permite salvar la prohibición general de tratar los datos relacionados con las opiniones políticas que el art. 9.1 impone, cuando el tratamiento sea efectuado por una fundación o asociación en el ámbito de sus actividades legítimas y con las debidas garantías [art. 9.2.d)]; cuando el interesado hubiera hecho manifiestamente públicos esos datos [9.2.e)]; o cuando se estime necesario "por razones de interés público esencial" [9.2.g)].

Al comentar el art. 8 de la derogada Directiva de protección datos 95/46/CE[14], Troncoso Reigada (2010: 37 y 75) advirtió que, el legislador europeo, al establecer las excepciones a la prohibición general de tratar determinadas categorías de datos, había utilizado conceptos abiertos e imprecisos que no ofrecían demasiada seguridad jurídica. A la misma conclusión llega García Sanz (2019: 133) cuando comenta las circunstancias habilitadoras del Considerando 56 RGPD: permitir que los partidos políticos puedan recopilar tal categoría de datos "en el marco de sus actividades electorales", "por razones de interés público" y cuando así lo exija "el funcionamiento del sistema democrático", lejos de ofrecer seguridad, genera incertidumbre pues son conceptos vagos e indeterminados. Cano Villalba (2022: 353) también comparte esta opinión. Recuérdese que el RGPD advierte que "el principio de transparencia exige que toda la información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro" (Considerando 58 y art. 5).

Fue esta falta de precisión en torno a las garantías lo que justificó la estimación del recurso de inconstitucionalidad contra el art. 58 bis, apdo. 1 de la LOREG. El legislador, señala el TC, debió de haber establecido garantías "de tipo técnico, organizativo y procedimental", al objeto de prevenir riesgos y de mitigar los efectos que se derivarían de un uso potencialmente invasor en los derechos de las personas. Sin tales garantías, advierte el TC, "los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental" no quedan "real, concreta y efectivamente protegidos" [FJ. 6, a)].

Apoyándose en la jurisprudencia del TJUE, el TC recuerda que la ley que limite este derecho debe de contemplar "unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos" [FJ. 6,

[14] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

b)][15], llegando a la conclusión de que el precepto impugnado "en absoluto" cumplía con esta condición. A mayor abundamiento, el TC también censura que la disposición impugnada: 1) permitiera que los partidos políticos pudieran recopilar esta categoría de datos "«en el marco de sus actividades electorales», otro concepto indeterminado que no tiene por qué coincidir con el periodo legalmente previsto en cada proceso de elecciones con la campaña electoral" [FJ. 6, c)]; 2) no identificara el interés público esencial que servía de base al tratamiento, esto es, el propósito que aquella recopilación de datos tenía; 3) y no contemplara regla alguna sobre el alcance y contenido de los tratamientos de datos autorizados, lo que impedía valorar la proporcionalidad de la injerencia sobre el derecho fundamental afectado (FJ. 7). Por estas razones, la STC 76/2019 estimó el recurso, esto es, porque la ley no precisó las garantías adecuadas, no, como advierte Rallo Lombarte (2019), porque la recopilación de datos personales relativos a las opiniones políticas por parte de los partidos políticos, en el marco de sus actividades electorales, fuera inconstitucional.

A la luz de esta sentencia, y de la más reciente STC 66/2022, de 2 de junio, FJ. 5, que se pronuncia en el mismo sentido, queda claro que el derecho a la protección de datos solo puede ser limitado por ley y con reglas claras y precisas que garanticen la seguridad y confidencialidad de los mismos, especificando con la suficiente claridad en qué casos se podría limitar el derecho, y las medidas restrictivas que pudieran ser implementadas. Así lo exigen el RGPD [arts. 9.2.g) y 22.4], la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales [art. 9.2], y también el art. 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que configura un régimen más o menos estricto en función de la naturaleza del dato protegido, siendo el máximo nivel de tutela el que se concede a las categorías de datos relacionados en el párrafo primero del art. 15.1 (los que "revelen la ideología, afiliación sindical, religión o creencias"), a los que no se podrá acceder a menos que el afectado consienta expresamente y por escrito, salvo que este los hubiese hecho manifiestamente públicos con anterioridad a la solicitud de acceso[16].

Con todo, parece que esta protección que descansa sobre la naturaleza del dato no es suficiente, pues una vez que los sistemas inteligentes son capaces de sacar conclusiones sobre las opiniones políticas de las personas a partir de información

[15] El TC se remite a la sentencia de la Gran Sala del TJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd*, apartado 54. En este apartado, el TJUE a su vez, se remite a las sentencias del TEDH en los casos *Liberty y otros c. Reino Unido* de 1 de julio de 2008, núm. 58243/00, parágrafos 62 y 63; *Rotaru c. Rumanía*, parágrafos 57 a 59; y *S y Marper c. Reino Unido*, parágrafo 99.

[16] El siguiente nivel de protección es el que concede el párrafo segundo del art. 15.1 (datos personales sobre el origen racial, salud, vida sexual, datos genéticos o biométricos o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor) a los que no se podrá acceder salvo consentimiento expreso del afectado o salvo que una norma con rango de ley lo permita. Como se habrá apreciado, estos datos coinciden esencialmente con los identificados en el art. 9.1 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

aparentemente neutral o de otra naturaleza, hay que actuar en consecuencia para reducir en lo posible el riesgo, de lo que nos ocupamos en los siguientes epígrafes.

4.- Sobre el riesgo cierto de que las nuevas tecnologías puedan interferir en los procesos de deliberación democrática

La capacidad que las nuevas tecnologías de la información y la comunicación tiene de interferir en los procesos democráticos de participación política viciando la libertad de expresión de los electores que el voto representa ha sido suficientemente advertida por la doctrina (entre otros, por Rodotà, 2003: 19; Troncoso Reigada, 2010: 73-74; Rubio, 2011: 319; García Mahamut, 2015: 309-338; Schwartz, 2019: 165; García Sanz, 2019: 134; o Villalba Cano, 2022: 357). Sin libertad de pensamiento no hay democracia, por eso urgen mecanismos que puedan advertir e invalidar esta clase de prácticas subrepticias contrarias a la Constitución. No faltan ejemplos que advierten la necesidad de fortalecer el sistema:

Quizá el caso con mayor trascendencia mediática hasta la fecha haya sido la filtración con fines políticos de millones de datos personales de los usuarios de Facebook a la consultora Cambridge Analytica, en beneficio de la campaña electoral de Donald Trump en las elecciones presidenciales de 2016. Pero no ha sido el único. Entre otros: en Brasil, en las elecciones presidenciales de 2018, días antes de que se eligiera al líder de la derecha, Jair Bolsonaro, el diario *Folha de S. Paulo* sacó a la luz un plan de tres millones de dólares para promocionar con mensajes virales e informes falsos a este candidato[17]; en India, varios grupos de la sociedad civil denunciaron campañas en internet y redes sociales (Facebook, Whatsaap) de desinformación en favor de Narendra Modi; la consultora arriba citada también intervino en Kenia en las elecciones que llevaron a la presidencia a Uhuru Kenyatta en 2013, diseñando una estrategia basada en el estudio de las necesidades de trabajo del electorado y en sus miedos relacionados con la violencia tribal, temas en los que se centró la campaña electoral del candidato, enviando a través de las redes sociales mensajes personalizados a los ciudadanos[18].

Garantizar el derecho a la protección de datos utilizando como criterio la naturaleza del dato ya no es suficiente. Los sistemas informáticos permiten la elaboración de perfiles que, sin utilizar las categorías especiales de datos en principio prohibidas por el art. 9.1 RGPD, permiten obtener información sensible sobre la persona. Por ejemplo, no es difícil, advierte Kahneman (2021: 36), conocer la ideología de una persona o su orientación sexual, combinando datos tan dispares como las salas de cine que visita, sus directores favoritos, los restaurantes que frecuenta, el barrio donde habita o sus respuestas ante determinados estímulos en las redes. Toda esta

[17] Noticia accesible en el Diario *El País* de 19 de octubre de 2018 con el titulo "Una investigación apunta a una gran trama de propaganda ilegal a favor de Bolsonaro por WhatsApp".

[18] Sobre estos casos, véase en la web de *Internet Health Report* el informe 2019 con el titulo "El desafío de la democracia en la era digital".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

información puede ser utilizada para viciar el pensamiento de millones de personas sobre sus decisiones en los procesos de participación política.

El TJUE así lo ha advertido en la cuestión prejudicial que resuelve la Gran Sala en la sentencia C-184/20, de 1 de agosto de 2022. El asunto a resolver era si "unos datos que pueden revelar, mediante un ejercicio intelectual de relación o deducción, la orientación sexual de una persona física, están comprendidos en las categorías especiales de datos personales en el sentido [...] del artículo 9, apartado 1, del RGPD" (apartado 120). La respuesta fue afirmativa: los datos que dejan al descubierto, de una manera indirecta, información sensible sobre una persona física también deben estar sometidos al régimen de protección reforzada del art. 9.1 RGPD, "pues de quedar fuera se menoscabaría el efecto útil de ese régimen y la protección de las libertades y de los derechos fundamentales de las personas físicas que pretende garantizar" (apartado 127).

A la vista de esta sentencia, los documentos o archivos públicos de los que puedan derivarse indirectamente datos sobre la ideología o creencias personales debieran de estar dotados de la misma protección que aquellos que revelan directamente tal información. Entre la doctrina, Medina Guerrero (2023: 63) se ha pronunciado en este sentido, advirtiendo la necesidad de abordar de manera decisiva las carencias de la normativa de protección de datos en lo referente a la regulación de los datos especiales. En la misma dirección, Jove Villares (2021: 329) constata que "el constante aumento de la capacidad para generar nuevas informaciones y datos personales, mediante la combinación de algoritmos, inteligencia artificial y *big data*, hace perentorio afrontar esta cuestión". También la Agencia Española de Protección de Datos lo advierte en el preámbulo de la Circular 1/2019: el "alto riesgo para los derechos y libertades de las personas físicas [es] difícilmente mitigable si no se toman medidas adecuadas".

Con esta finalidad de extremar las precauciones, consideramos que efectivamente sería recomendable una modificación del sistema de protección para que este no bascule exclusivamente sobre la naturaleza sensible de los datos (art. 9.1 RGPD) sino que atienda principalmente a la finalidad que justifique el tratamiento. Entendemos que esta es la posición del *Reglamento de IA*, que no permite la utilización de estas técnicas cuando ello provoque "un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos enteros de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente" [art. 5.1.c).i)].

La elaboración de perfiles y las decisiones automatizadas es algo frecuente en un número creciente de sectores, tanto públicos como privados[19]. Que estas estrategias

[19] En España se ha generalizado el uso de sistemas algorítmicos de apoyo para la toma de decisiones en la Administración Pública. Sin embargo, la escasa información sobre el funcionamiento de los algoritmos y la complejidad de los sistemas de inteligencia artificial dificultan el control de los actos administrativo automatizados, limitando la capacidad de los ciudadanos para recurrir tales decisiones (Jiménez-Castellanos Ballesteros, 2023: 191-215). A ello hay que unir que el uso y el tratamiento de los datos personales mediante la implementación de la inteligencia artificial conlleva riesgos distintos

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

basadas en la lógica matemática y el conocimiento no ignoren los principios y valores que fundamentan nuestro modelo constitucional de convivencia y que las garantías que al efecto se contemplen no animen a los agentes que desarrollan esta industria a buscar puertos más seguros para sus intereses es el principal reto que el Derecho tiene por delante. En esta empresa parece evidente que la regulación nacional no es suficiente. La realidad de este fenómeno exige un marco legal uniforme que garantice la operatividad de sus disposiciones (Girón Reguera, 2023:443-44).

A este desafío se enfrenta el *Reglamento de IA*, que reconociendo que el uso de estas técnicas puede tener repercusiones negativas para múltiples derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, responde garantizando un elevado nivel de protección para dichos derechos fundamentales (…) sirviéndose de un conjunto de requisitos destinados a conseguir que la IA sea fiable y que se impongan obligaciones proporcionadas a todos los participantes en la cadena de valor[20]. También la Resolución sobre la inteligencia artificial en la era digital, de 3 de mayo de 2022 [2020/2266(INI)], ha insistido en la necesidad apremiante de plantear una estrategia conjunta en el seno de la UE, pero recordando que "para generar confianza en la inteligencia artificial entre los ciudadanos, sus derechos fundamentales deben de protegerse en todos los aspectos de la vida, también en el contexto del uso de la inteligencia artificial en la esfera pública y en el lugar de trabajo" (parágrafo 302).

5.- Algunas medidas que pudieran reducir el riesgo de manipulación política a partir del tratamiento inteligente de los datos personales

La necesidad de aumentar los niveles de transparencia de la publicidad política queda patente en el *Reglamento del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre la transparencia y segmentación en la publicidad política*[21]. Su Considerando 74 reconoce que cada vez es más frecuente el uso de datos personales recogidos directamente de las personas, o indirectamente a partir de su actividad en línea, para la elaboración de perfiles de comportamiento y otras técnicas de análisis, "para orientar los mensajes políticos hacia grupos o votantes individuales y para amplificar su impacto". Al efecto, continúa este Considerando, hay que ser conscientes de que "a partir del tratamiento de datos personales, en particular [de] las categorías especiales de datos personales con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725, es posible segmentar diferentes grupos de votantes o individuos [para] aprovechar sus características o vulnerabilidades, por ejemplo, difundiendo los anuncios en momentos y lugares específicos concebidos para sacar partido de las situaciones en que serían sensibles

frente a los derivados de un tratamiento que pueda realizar cualquier otro responsable, como ha advertido la Agencia Española de Protección de Datos (2023).

[20] *Diario Oficial de la Unión Europea*, núm. 900, de 20 de marzo de 2024, pp. 1-44.

[21] COM(2021) 731 final. 2021/0381 (COD). Bruselas, 25 de noviembre de 2021.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

a un determinado tipo de información o mensaje". Este tipo de tratamientos personales, prosigue el Considerando, "tiene efectos específicos y perjudiciales para los derechos y libertades fundamentales de las personas (…) [además de repercutir] negativamente en el proceso democrático, puesto que conduce a la fragmentación del debate público sobre cuestiones sociales importantes, la actividad de acercamiento selectivo y, en última instancia, la manipulación del electorado. También aumenta el riesgo de propagación de la manipulación de la información y la injerencia exterior. La publicidad política engañosa o encubierta constituye un riesgo pues influye en los mecanismos básicos que permiten el funcionamiento de nuestra sociedad democrática". Por todo ello –concluye- "deben establecerse restricciones y condiciones adicionales en comparación con las establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725".

Por su parte, la Comisión Europea también ha expresado su preocupación al respecto en las siguientes Comunicaciones: en El *Plan de Acción para la Democracia Europea* [22] ha reclamado "la necesidad de una mayor transparencia en la publicidad política y la comunicación y en las actividades comerciales que la rodean, a fin de que los ciudadanos, la sociedad civil y las autoridades responsables sean capaces de ver claramente el origen y la finalidad de dicha publicidad"; y en otras dos que llevan el título *La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos* (de 24 de junio de 2020)[23] y *La lucha contra la desinformación en línea: un enfoque europeo* (de 26 de abril de 2018)[24], también ha advertido que la desinformación es una herramienta que puede ser utilizada para manipular los procesos electorales. La última de las citadas, alerta concretamente del uso de las redes sociales y de las nuevas tecnologías "para difundir desinformación a gran escala y con una velocidad y una precisión de selección de los destinatarios sin precedentes, de modo que permiten crear esferas de información personalizadas y se convierten en poderosas cámaras de resonancia para las campañas de desinformación". Estas prácticas, advierte el citado texto, erosionan "la confianza en las instituciones y en los medios de comunicación digitales y tradicionales y perjudica a nuestras democracias, obstaculizando la capacidad de los ciudadanos de tomar decisiones informadas" [25].

En la medida en que el tratamiento inteligente de los datos permite construir estrategias o procedimientos para analizar a cada persona en particular con el

[22] *Plan de Acción para la Democracia Europea*, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM/2020/790 final), de 3 de diciembre de 2020.

[23] COM(2020) 264 final], Bruselas, 24 de junio de 2020, p. 4.

[24] COM(2018) 236 final, de 26 de abril de 2018, p. 13.

[25] Doc. COM(2018) 236 final, Introducción. Accesible en: http://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-236-F1-ES-MAIN-PART-1.PDF.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

objetivo de influir en sus decisiones políticas, los poderes públicos tienen la obligación positiva de actuar en consecuencia, estableciendo mecanismos que garanticen la transparencia y legalidad de tales prácticas. En un entorno en línea personalizado y microsegmentado no es difícil polarizar política e ideológicamente a los ciudadanos para influir en su decisión de voto, advierte el Supervisor Europeo de Protección de Datos Supervisor Europeo de Protección de Datos (2018: C 233/10).

Resulta, pues, perentorio prestar una mayor "atención jurídica" al uso masivo y tratamiento ilegítimo de los datos personales en este ámbito de la política (García Mahamut, 2015: 324). Monitorizar y, en su caso, controlar la difusión de mensajes falsos podría ser una de las soluciones, aunque, como advierte Serra Cristobal (2023: 46), ello conlleve un riesgo evidente para la libertad de expresión. Lo que no es razonable es que la LOREG no contenga ninguna disposición que haga referencia a la publicidad electoral en el entorno de internet, como también ha denunciado García Mahamut (2023: 95), o que la Junta Electoral no disponga de los medios necesarios para garantizar la transparencia, la objetividad y el principio de igualdad de la campaña electoral en ese contexto, como han lamentado García Sanz (2019: 134) y Sánchez Muñoz (2020: 278).

Si bien algún autor ha cuestionado que el perfilado ideológico y la microsegmentación electoral puedan tener la capacidad suficiente como para influir en la decisión de los votantes (en este sentido, Hernández Peña, 2022: 69), los textos de la Unión Europea citados al inicio de este epígrafe y la opinión que estimamos mayoritaria entre la doctrina advierten del posible uso de estas prácticas para cambiar el sentido del voto de los electores mediante el envío de mensajes a medida; de la capacidad que el tratamiento de datos tiene para manipular a segmentos enteros de la población con el objetivo de interferir en los procesos democráticos (García Sanz, 2019: 144); de que los datos pueden ser utilizados para entender el comportamiento de las personas y utilizar tal información en beneficio de intereses espurios; y de que esta propaganda electoral soterrada es la más peligrosa (Jason, 2015:46).

Entre las medidas posibles para reducir el riesgo, quizá pudiera ser contemplada la modificación del art. 22 RGPD, que prohíbe el "tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en [el interesado] o le afecte significativamente de modo similar". Como vemos, el precepto exige tres requisitos acumulativos: que se trate de una «decisión»; que esta esté «basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles», y, por último, que produzca «efectos jurídicos» u otros que le afecten «significativamente de modo similar»". La modificación iría en el sentido de que tal prohibición no se circunscriba exclusivamente a las decisiones o elaboración de perfiles que produzcan efectos jurídicos o similares *ad personam*, sino también a otra clase de prácticas que puedan afectar a toda la comunidad política, como las que tratan de manipular la decisión de los ciudadanos en unos comicios electorales, como Arenas Ramiro (2019: 371) también advierte.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

Dado que los algoritmos y la inteligencia artificial tienen la capacidad de realizar una labor muy productiva a este respecto, examinando el comportamiento del ciudadano en la Red, para a partir de ahí diseñar una estrategia personalizada de captación del voto (Kosinski *et al*., 2013), el ordenamiento jurídico debiera estar dotado de instrumentos que pudieran neutralizar tales amenazas de manera inmediata. Así lo advierte el *Reglamento de IA* en su Considerandos 28: esta tecnología, utilizada de manera indebida, puede proporcionar "nuevas y poderosas herramientas para llevar a cabo prácticas de manipulación, explotación y control social. Dichas prácticas son sumamente perjudiciales e incorrectas y deben estar prohibidas, pues van en contra de los valores de la Unión de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y de los derechos fundamentales consagrados en la Carta, como el derecho a la no discriminación, a la protección de datos y a la intimidad y los derechos del niño". Modificar el art. 22.1 RGPD en el sentido propuesto consideramos que podría ayudar a aminorar este riesgo, pues con la redacción actual, como recientemente ha recordado la sentencia del TJUE de 7 de diciembre de 2023 en el asunto C-634/21 (*OQ c. Land Hessen*), la prohibición solo afecta a los tratamientos que afecten singularmente al interesado.

Es cierto que el tratamiento de datos personales sobre opiniones políticas está prohibido, con carácter general, en el art. 9.1 RGPD, pero entendemos que la apertura del art. 22 RGPD en el sentido apuntado podría ser de utilidad para impedir el perfilado ideológico a partir de datos que, siendo aparentemente neutrales, combinados con otros podrían ser utilizados para estudiar el comportamiento del elector con la finalidad de modificar su voto. En cuanto que los resultados de unas elecciones, de una u otra manera, terminan produciendo efectos jurídicos en el interesado, la modificación de este precepto en el sentido apuntado podría, a nuestro parecer, contribuir a reducir el riesgo evidente de que esta tecnología se utilice de manera fraudulenta para moldear la opinión política de los ciudadanos.

6.- Recapitulación

El artículo 18.4 CE ordena al legislador que proteja los derechos de las personas frente al uso de la informática. En este precepto, el Tribunal Constitucional ha reconocido el derecho fundamental a la protección de datos personales, al que le asigna un contenido sustantivo propio. Por su evidente relevancia en el contexto digital que las tecnologías de la información y la comunicación están generando, este derecho debería estar expresamente reconocido en la Constitución, pues se trata de una herramienta imprescindible para el pleno ejercicio de los derechos fundamentales en el entorno de internet. Por la misma razón, el derecho de acceso a la información pública y a la transparencia, que el art. 105 b) CE reconoce, debiera ser concebido como derecho fundamental, dada su directa relación con la libertad de información, tal y como ha reconocido el TEDH. La negación de "la más mínima relación" entre ambos, que declara la sentencia 140/2023, de 7 de febrero, del Tribunal Supremo (Sala de lo Contencioso-Administrativo), ignorando esta

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

jurisprudencia (art. 10.2 CE), puede ser una señal sobre la necesidad de actualizar la configuración constitucional del mismo.

Hay que preparar la Constitución frente a los retos más desafiantes de la era digital. Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Este nuevo entorno exige, no solo actualizar los derechos que en la Constitución están reconocidos sino también incorporar otros que puedan dar respuesta a las amenazas que brotan de este nuevo mundo, tal y como advierte el apartado IV del Preámbulo de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. En esa dirección, el Gobierno de España adoptó, en julio de 2021, la Carta de Derechos Digitales, y la Unión Europea, en diciembre de 2022, la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital.

El tratamiento de datos personales debe de realizarse en condiciones de transparencia, por ello el legislador ha de establecer mecanismos que permitan a los jueces controlar que los datos recopilados no sean utilizados para fines distintos para los que fueron solicitados. En relación con esta supervisión, hay quienes advierten que un exceso de protección de algunos de los principios relativos al tratamiento, particularmente el principio de limitación de la finalidad y el de minimización de datos, podría ralentizar los avances que las nuevas tecnologías ofrecen. Este desarrollo, empero, no puede menoscabar los derechos y libertades de las personas. El bien jurídico protegido por el derecho a la protección de datos son todos los derechos de las personas que pudieran verse comprometidos por un uso ilegítimo de aquellos. Una manera de hacerlo es permitir que los ciudadanos puedan supervisar las decisiones automatizadas que les afecten, lo que no será posible sin información sobre los algoritmos utilizados.

Si bien este derecho fundamental concede al interesado un haz de facultades para ejercer el control sobre los datos que le conciernen, la práctica demuestra que no se trata de una garantía suficiente, pues el titular, por sí solo, es incapaz de hacer frente a toda esta tecnología que permite el uso cotidiano y a escala masiva de sus datos personales. La opacidad de los procedimientos que tienen que ver con el tratamiento de nuestros datos justifica una sensación generalizada de inseguridad que los poderes públicos deben de afrontar cumpliendo con la obligación positiva de proteger los derechos de las personas. Como ha señalado la STC 79/2019, FJ. 6. A), son necesarias garantías adecuadas "de tipo técnico, organizativo y procedimental", pues sin ellas, los intereses jurídicamente protegibles no quedarán "real, concreta y efectivamente protegidos".

El sesgo discriminatorio en las decisiones automatizadas es una de las amenazas más evidentes. El *Reglamento de Inteligencia Artificial*, aprobado el 13 de marzo de 2024, advierte expresamente sobre la urgencia de abordar esta cuestión. Los derechos de las personas deben estar protegidos frente a las estrategias que la tecnología de la Inteligencia Artificial permite implementar. A tales efectos deben habilitarse procedimientos para que los ciudadanos puedan supervisar los procesos

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 19. Primer semestre. Enero-junio 2024
www.revistatransparencia.com

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

de toma de decisiones que les afecten. El empleo de la lógica matemática debe ajustarse a los parámetros constitucionales.

Es necesario aumentar los niveles de transparencia al objeto de que toda la información relativa al tratamiento de los datos personales sea efectivamente fácilmente accesible y fácil de entender, siendo conscientes de que dada la capacidad que tiene la Inteligencia Artificial de sacar conclusiones, el foco de atención parece que no puede quedar centrado exclusivamente en la naturaleza del dato (artículo 9.1 RGPD) sino también sobre el resultado que el tratamiento pueda generar.

En esta misma dirección, entendemos que el art. 22 RGPD no debiera prohibir tan solo la elaboración de perfiles que produzcan efectos jurídicos en el interesado o le afecten significativamente de manera similar. A nuestro juicio, esta prohibición no debiera ceñirse exclusivamente a las decisiones que produzcan efectos *ad personam* sino también a aquellas que puedan influir en el funcionamiento del sistema democrático. En un entorno en línea personalizado y microsegmentado hay que articular mecanismos que reduzcan el riesgo de polarizar la sociedad y de manipular la voluntad del elector a partir del análisis de su comportamiento. En esta dirección, evitar conceptos jurídicos vagos o indeterminados a la hora limitar la posible recopilación de datos por parte de las fuerzas políticas al objeto de diseñar sus campañas electorales (Considerando 56 RGPD) resulta también imprescindible. El legislador (nacional e internacional) debe de especificar con la suficiente claridad los supuestos en los que un derecho pueda ser limitado y las medidas que al efecto puedan ser implementadas. Entre ellas, monitorizar y, en su caso, controlar la difusión de mensajes falsos puede ser una posibilidad, aunque estableciendo las garantías adecuadas para reducir el riesgo evidente para la libertad de expresión. Hoy la propaganda electoral no siempre es explícita.

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

Bibliografía

ARENAS RAMIRO, M. 2019. "Partidos políticos, opiniones políticas e internet: la lesión del derecho a la protección de datos personales". Teoría y Realidad Constitucional, n. 44, pp. 341-372.

BILBAO UBILLOS, J. M. 2019. "Ponente", en RODRÍGUEZ, A. (Coord.). *40 años de Constitución: una mirada al futuro*, *Actas del XVI Congreso de la Asociación de Constitucionalistas de España*. Valencia: Tirant lo Blanch, pp. 65-112.

BLANES CLIMENT, M. A. 2023. "El derecho fundamental a la libertad de información y el derecho de acceso a la información pública (STS 7/2/2023)", 13 marzo 2023, *Blog de Transparencia y Gobierno Abierto* (https:/miguelangelblanes.com).

CARRILLO, M. 2015. "Transparencia y derechos de acceso a la información en las administraciones públicas". *Parlamento y Constitución. Anuario*, núm. 17, pp. 267-284.

COTINO HUESO, L. 2017. "El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental". *Teoría y Realidad Constitucional*, núm. 40, pp. 279-316.

DÍEZ PICAZO, L. M. 2005, *Sistema de derechos fundamentales*. Madrid: Thomson & Civitas.

FERNÁNDEZ RAMOS, S. y PÉREZ MONGUIÓ, J. M. 2017. *El derecho al acceso a la información pública en España*, Cizur Menor: Thomson/Aranzadi.

GARCÍA MAHAMUT, R. 2023. "Elecciones, protección de datos y transparencia en la publicidad política: la apuesta normativa de la UE y sus efectos en el ordenamiento español". *Revista Española de la Transparencia*, núm. 17, pp. Págs. 75-105. DOI: https://doi.org/10.51915/ret.307

- (2015) "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español". *Teoría y Realidad Constitucional*, núm. 35, pp. 309-338.

GARCÍA SANZ, R. M. 2019. "Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público". *Revista de Estudios Políticos*, núm. 183, pp. 129-159.

GIRÓN REGUERA, E. 2023. "La regulación jurídica de la inteligencia artificial como garantía de los derechos: su protección en la futura Ley Europea de Inteligencia Artificial", en LÓPEZ ULLA, J. M. (Dir.), *El impacto de la era digital en el Derecho*. Cizur Menor: Aranzadi, pp. 441-469.

HERNÁNDEZ PEÑA, J. C. 2022. "Campañas electorales, big data y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos". Revista Española de Derecho Constitucional, núm. 124, pp. 41-73. doi: https://doi.org/10.18042/cepc/redc.124.02

JASON, S. 2015. *How Propaganda Works*. New Jersey: Princeton University.

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

JIMÉNEZ-CASTELLANOS BALLESTEROS, I. 2023. "Decisiones automatizadas y transparencia administrativa: nuevos retos para los derechos fundamentales". *Revista Española de la Transparencia*, núm. 16, pp. 191-215. DOI: https://doi.org/10.51915/ret.250

JOVE VILLARES, D. 2021. "La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de mayo", *Revista Española de Derecho Constitucional*, núm. 121: 303-331.

KAHNEMAN, D., SIBONY O., & SUNSTEIN C. 2021. *Ruido: Un fallo en el juicio humano*, Santiago de Chile: Penguin Random House.

KOSINSKI, M., STILLWELL, D. y GRAEPEL, T. M. 2013. Private traits and attributes are predicable from digital records of human behavior. Proceedings of the National Academy of Sciences, 110 (15), pp. 5802-5805. DOI: https://doi.org/10.1073/pnas.1218772110.

LÓPEZ AGUILAR, J. F. 2023. "Transparencia, un derecho europeo, y su relación con otros bienes constitucionalmente relevantes", *Revista Española de la Transparencia*, núm. 17, pp. 23-49. DOI: https://doi.org/10.51915/ret.305

LÓPEZ ULLA, J. M. 2021. "La libertad de expresión y el derecho de rectificación en la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (Comentario al art. 85 LOPDGDD)", en TRONCOSO REGIADA, A. (Dir). *Comentarios al Reglamento General de Protección de Datos y a Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*, Tomo I, Civitas Thomson Reuters, pp. 4007-4030.

MEDINA GUERRERO, M. 2023. "El conflicto entre la transparencia y la protección de datos tras la entrada en vigor del Reglamento General de Protección de Datos". *Revista Española de la Transparencia*, núm. 17, pp. 51-73.

- (2022) "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales". *Teoría y realidad constitucional*, núm. 49, pp. 141-171.

RALLO LOMBARTE, A. 2019. "La LOPDGDD y el art. 58 bis LOREG". *Diario La Ley*, n. 34, 5 de diciembre de 2019.

- (2017) "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet". *Teoría y Realidad Constitucional*, núm. 39, pp. 583-610.

REY MARTÍNEZ, F. 2014. "*Quod omnes tangit ab omnibus cognitum es-se debet*: el derecho de acceso a la información pública como derecho fundamental", *Revista Jurídica de Castilla y León*, núm. 33, pp. 19-26.

REVENGA SÁNCHEZ, M. 2023. "El tiempo de los derechos en la era digital", en LÓPEZ ULLA, J. M. (Dir.), *El impacto de la era digital en el Derecho*. Cizur Menor: Aranzadi, pp. 37-54.

RODOTÀ, S. 2003. "Democracia y protección de datos", *Cuadernos de Derecho Público*, núm. 19-20, pp. 15-26.

Sección Estudios y Artículos
Garantías adecuadas para proteger la democracia frente al uso fraudulento de los datos personales
por Juan Manuel López Ulla
Págs. 71-93
DOI: https://doi.org/10.51915/ret.343

RUIZ-RICO RUIZ, G. 2021. "La dimensión constitucional del principio de transparencia y el derecho de información activa". *Revista de Derecho Político* núm. 110, pp. 47-78.

SÁNCHEZ BARRILAO, J. F. 2016. "El derecho constitucional ante la era de ultrón: la informática y la inteligencia artificial como objeto constitucional". *Estudios de Deusto*, Vol. 64/2, pp. 225-258.

SÁNCHEZ MUÑOZ, O. 2020. *La regulación de las campañas electorales en la era digital. Desinformación y microsegmentación en las redes sociales con fines electorales*, Madrid: Centro de Estudios Políticos y Constitucionales.

SCHWARTZ, P.M. (2019). "Privacy and Democracy in Cyberspace", *Vanderbilt Law Review*, Vol. 52, pp. 1610-1701.

SERRA CRISTOBAL, R. 2023. "Noticias falsas (fakes news) y derecho a recibir información veraz. dónde se fundamenta la posibilidad de controlar la desinformación y cómo hacerlo". *Revista de Derecho Político*, núm. 116, pp. 13-46.

Supervisor Europeo de Protección de Datos. 2018. "Opinion 3/2018, Opinion on online manipulation and personal data". 19 de marzo de 2018. *Diario Oficial de la Unión Europea*, 4 de julio de 2018, C 233/10.

TRONCOSO REIGADA, A. 2023. "El derecho a la garantía de la confidencialidad e integridad de los sistemas de tecnologías de la información: un ejemplo de nuevo derecho digital", en LÓPEZ ULLA, J. M. (Dir.), *El impacto de la era digital en el Derecho*. Cizur Menor: Aranzadi, pp. 239-281.

- (2019) "Presentación", en TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Civitas, pp. 71- 74.

RUBIO NÚÑEZ, R. 2011. "Nuevas tendencias de regulación del uso de las nuevas tecnologías en campaña electoral", en BARRAT I ESTEVE, J. y FERNÁNDEZ RIVEIRA, R. (coords.). *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías*. Pamplona: Thomson Reuters, pp. 313-333.

VELASCO RICO, C.I. 2022. "Las tecnologías disruptivas en la administración pública: Inteligencia Artificial y Block Chain", en coord. CASTILLO RAMOS-BOSSINI, S.E y CERRILLO I MARTÍNEZ, A (Dirs.), *La Administración digital*. Madrid: Dykinson. pp. 227-256.

VILLALBA CANO, L. 2022. *El derecho fundamental a la protección de datos personales en el constitucionalismo multinivel europeo: su contenido esencial*. Tesis doctoral. Universidad de Cádiz.

VILLAVERDE MENÉNDEZ, I. 2019. "El marco constitucional de la transparencia". *Revista Española de Derecho Constitucional*, núm. 116, pp. 167-191. doi: https://doi.org/10.18042/cepc/redc.116.06