#RET

Revista Española de la Transparencia
Núm. 17. Número extraordinario 2023
ISSN 2444-2607 www.revistatransparencia.com

Monográfico sobre la protección de datos y su conciliación con la transparencia y la lucha contra la corrupción

Coordinación del número extraordinario:

Rosario García Mahamut

Beatriz Tomás Mallén

Este número se ha financiado con el proyecto «La conciliación del derecho a la protección de datos con el cumplimiento por los poderes públicos del deber de transparencia y de lucha contra la corrupción (DATATRANSCO)» (referencia: PID2021-128309NB-I00) del Ministerio de Ciencia e Innovación.

CC BY SA

#RET

Revista Española de la Transparencia

ISSN 2444-2607
Depósito Legal: MU 533-2015

La REVISTA ESPAÑOLA DE LA TRANSPARENCIA (#RET) es una publicación digital de periodicidad semestral que sirve a la divulgación, análisis, debate e intercambio académico y profesional en relación a la transparencia y campos afines como la participación y la rendición de cuentas en el marco del Gobierno Abierto y el Buen Gobierno.

Monográfico dedicado a la protección de datos y su conciliación con la transparencia y la lucha contra la corrupción

Este número se ha financiado con el proyecto «La conciliación del derecho a la protección de datos con el cumplimiento por los poderes públicos del deber de transparencia y de lucha contra la corrupción (DATATRANSCO)» (referencia: PID2021-128309NB-I00) del Ministerio de Ciencia e Innovación.

EDITA:
ACREDITRA. Asociación de Profesionales de la Transparencia
C/ Esparto, 2 - 30600 Archena. Murcia. España
Registro Nacional de Asociaciones: Grupo 1º / Sec. 1ª / N.º Nacional: 604676
CIF: G73832156
E-mail: info@revistatransparencia.com

IMAGEN DE PORTADA: canva.com

ACCESO ABIERTO, CONTENIDOS, LICENCIA Y DIFUSIÓN:
Acceso abierto a sus contenidos en: www.revistatransparencia.com

La REVISTA ESPAÑOLA DE LA TRANSPARENCIA (#RET) no se hace responsable de las opiniones de los colaboradores que las expresarán, en todo momento, de manera individual y en caso alguno representando la opinión de la revista. La opinión de la REVISTA ESPAÑOLA DE LA TRANSPARENCIA (#RET) sólo se refleja en el Editorial.

La REVISTA ESPAÑOLA DE LA TRANSPARENCIA (#RET) está bajo licencia Creative Commons Reconocimiento-Compartir Igual 4.0 Internacional License.

Los artículos publicados pueden ser incluidos en repositorios y difundidos libremente sin restricción alguna.

Redes sociales:
Twitter: @RETransparencia
Academia: https://independent.academia.edu/RevistaEspañoladelaTransparenciaRET

EQUIPO DE DIRECCIÓN

Director:
Luis Alberto Gálvez Muñoz
Universidad de Murcia. España

Subdirector académico:
Javier Sierra Rodríguez
UNED. España

Subdirector de divulgación:
Francisco Delgado Morales
Asociación de Profesionales de la Transparencia (ACREDITRA). España

Secretaria:
Ana Galdámez Morales
Asociación de Profesionales de la Transparencia (ACREDITRA). España

Equipo de gestión del proceso editorial:

Milagrosa Bascón Jiménez. Universidad de Córdoba. España
Pablo Cruz Mantilla de los Ríos. Universidad Pompeu Fabra. España
Ricardo Curto Rodríguez. Universidad de Oviedo. España
María Diez Garrido. Universidad de Valladolid. España
Alicia González Moro. Universidad de Sevilla. España
Daniel Jove Villares. Universidad de La Coruña. España
Gabriel López Martínez. Universidad de Alicante. España
María Dolores Montero Caro. Universidad de Córdoba. España
Eloísa Pérez Conchillo. Universidad de Granada. España
Gabriele Vestri. Universidad de Cádiz. España

CONSEJO EDITORIAL

Rafael Ayala González. *Gobierno Transparente. España*

Rafael Camacho Muñoz. *Transparencia en España.*

Arrate García Campos. *Ibatuz. España*

Rosario Lopaz Pérez. *Acreditra..España*

Cuca Sacristán Sánchez. *Consultora CIAT. España*

EVALUADORES 2022

Listado de evaluadores correspondiente a los números publicados en el año 2022
(orden alfabético de apellidos)

Pablo Alarcón Peña
Universidad Espíritu Santo (Ecuador)

David Almagro Castro
Universidad de Sevilla. España

Adrián Ballester Espinosa
Universidad de Alicante. España

Concepción Barrero Rodríguez
Universidad de Sevilla. España

Miguel Ángel Blanes Climent
Sindic de la Comunidad Valenciana. España

Antonio Juan Briones Peñalver
Universidad Politécnica de Cartagena. España

Oscar Capdeferro Villagrasa
Universitat de Barcelona. España

Jorge Castellanos Claramunt
Universidad de Valencia. España

Agustí Cerrillo Martínez
Universidad Oberta de Catalunya. España

Juan Carlos Covilla Martínez
Universidad Externado de Colombia

Iria da Cunha Fanego
UNED. España

Carmen Gloria Droguett González
Universidad Andrés Bello (Chile)

Ángel Fernández Silva
Universidad de Salamanca. España

Pamela Figueroa Rubio
Universidad de Santiago de Chile

Jesús García García
Universidad de Oviedo. España

Verónica Yazmín García Morales
Universitat de Barcelona. España

José María Gimeno Feliú
Universidad de Zaragoza. España

Alejandro Gómez Velásquez
Universidad EAFIT (Colombia)

Juan González Ayesta
Universidad de Oviedo. España

Álvaro González-Juliana Muñoz
Universidad Pompeu Fabra. España

Pilar Lourdes González Torre
Universidad de Oviedo. España

Marcos Gutiérrez Ayala
Benemérita Universidad Autónoma de Puebla (México)

Mónica Martínez López-Sáez
Universidad de Valencia. España

Andrés Martínez Moscoso
Universidad San Francisco de Quito (Ecuador)

Lluís Medir Tejado
Universitat de Barcelona. España

Joaquín Meseguer Yebra
Ayuntamiento de Madrid. España

María Dolores Montero Caro
Universidad de Córdoba. España

Arancha Moretón Toquero
Universidad de Valladolid. España

Elisa Moreu Carbonell
Universidad de Zaragoza. España

Adriana Mutu
ESIC. España

Marta Oller Rubert
Universidad Jaume I. España

Emilio Oñate Vera
Universidad Central (Chile)

Víctor Peña Mancillas
Colegio de Sonora (México)

Camilo Perdomo Villamil
Universidad del Externado (Colombia)

Esther Rando Burgos
Universidad de Málaga. España

Gerardo Ruiz-Rico Ruiz
Universidad de Jaén. España

Mª Isabel Serrano Maillo
Universidad Complutense de Madrid. España

María Eugenia Suárez Serrano
Universidad de Oviedo. España

José Antonio Tardío Pato
Universidad Miguel Hernández. España

María Eugenia Teijeiro Lillo
Universidad de Cádiz. España

Raquel Valle Escolano
UNIR. España

Manuel Villoria Mendieta
Universidad Rey Juan Carlos. España

Diego Zalbidea González
Universidad de Navarra. España

CONSEJO ASESOR

José Manuel Canales Aliende
Universidad de Alicante
España

Rosario García Mahamut
Universidad Jaime I de Castellón
España

Marcos Gutiérrez Ayala
Benemérita Universidad Autónoma de Puebla. México

Esther Martínez Pastor
Universidad Rey Juan Carlos
España

Mariana Moranchel Pocaterra
Universidad Autónoma Metropolitana de México

Joan Oliver Araujo
Universidad de las Islas Baleares
España

José María Pérez Monguió
Universidad de Cádiz
España

Jesús Pérez Viejo
UNED
España

Edwin Cuitláhuac Ramírez Díaz
Universidad Nacional Autónoma de México

Fernando Reviriego Picón
UNED
España

Luis Efrén Ríos Vega
Universidad Autónoma de Coahuila
México

Catalina Ruíz-Rico Ruíz
Universidad de Jaén
España

Manuel Sánchez de Diego Fernández de la Riva
Universidad Complutense de Madrid. España

Isabel Serrano Maillo
Universidad Complutense de Madrid. España

Irene Spigno
Universidad de Siena
Italia

Anna M. Sroka
Universidad de Varsovia
Polonia

Antonio Torres del Moral
UNED
España

Crossref

ÍnDICEs
CSIC

Dialnet

latindex
catálogo

DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS

MIAR

DULCINEA

REDIB
Red Iberoamericana
de Innovación y Conocimiento Científico

ERIHPLUS
EUROPEAN REFERENCE INDEX FOR THE
HUMANITIES AND SOCIAL SCIENCES

Scopus

BY
SA

FECYT-527/2022
Fecha de certificación: 7ª Convocatoria (2021)
Válido hasta: 22 de julio de 2023

Contenido

Presentación del número monográfico dedicado a la protección de datos y su conciliación con la transparencia y la lucha contra la corrupción *17*
por José Luis Rodríguez Álvarez

Transparencia, un derecho europeo, y su relación con otros bienes constitucionalmente relevantes *23*
por Juan Fernando López Aguilar

El conflicto entre la transparencia y la protección de datos tras la entrada en vigor del Reglamento General de Protección de Datos *51*
por Manuel Medina Guerrero

Elecciones, protección de datos y transparencia en la publicidad política: la apuesta normativa de la UE y sus efectos en el ordenamiento español *75*
por Rosario García Mahamut

Transparencia algorítmica en los medios de comunicación y las plataformas digitales *107*
por Cristina Pauner Chulvi

Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales *137*
por Ana Garriga Domínguez

Transparencia pública, genoma y datos genéticos *165*
por Jesús Jiménez López

Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso? *201*
por David Díaz Lima

Las obligaciones de transparencia de las Autoridades de protección de datos: un requisito indispensable para su independencia..... *227*
por Mónica Arenas Ramiro

Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023: un derecho en vías de consolidación.....*271*
por Jorge Viguri Cordero

Las bases de datos y el data mining como herramientas contra la corrupción en la administración local.....*299*
por Jaime Clemente Martínez

CC BY SA

CONTRIBUCIONES

Convocatoria para la recepción de artículos

permanentemente abierta

Revista indexada en SJR-SCOPUS

Sello de calidad editorial FECYT y mención de buenas prácticas editoriales en igualdad de género

Consulte las directrices para el envío de originales en:

www.revistatransparencia.com

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Presentación

José Luis Rodríguez Álvarez

Presidente del Consejo de la Transparencia y Buen Gobierno

RESUMEN: Presentación del número monográfico dedicado a la protección de datos y su conciliación con la transparencia y la lucha contra la corrupción.

PALABRAS CLAVE: transparencia, protección de datos, corrupción, número monográfico.

Presentation

ABSTRACT: Presentation of the monographic issue dedicated to data protection and its reconciliation with transparency and the fight against corruption.

KEYWORDS: transparency, data protection, corruption, monographic issue.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

La edición de este número extraordinario de la *Revista Española de Transparencia* no podía ser más oportuna. En pocas semanas se cumplirán diez años de la aprobación por las Cortes Generales de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG), publicada en el Boletín Oficial del Estado (BOE) el 10 de diciembre de 2013. Celebro pues la iniciativa y agradezco a la profesora García Mahamut su amable y generosa invitación a escribir unas líneas introductorias.

El principio de transparencia ocupa hoy en día un lugar central en la configuración política de los Estados que se definen como democracias avanzadas, hasta el punto de que es comúnmente aceptado que el grado de transparencia efectiva de la actividad pública existente en cada país es un indicador muy fiable de su nivel de calidad democrática.

Ello es así porque la transparencia de la actuación de los poderes públicos, sin sustituir los tradicionales instrumentos de participación y de control propios de los sistemas políticos democráticos, los complementa y los refuerza considerablemente. Al demandar de las instituciones y de sus responsables una rendición de cuentas directa y permanente a la ciudadanía, instaura un cualificado canal de relación entre gobernantes y gobernados en el que la comunicación se materializa directamente, sin necesidad de intermediarios (como sucede con la que se articula a través de representantes políticos); y su vigencia no se circunscribe a momentos o procesos temporalmente acotados (como pueden ser los períodos electorales), sino que ofrece un cauce permanente para la interacción, disponible sin interrupciones.

Como es conocido, el principio de transparencia se despliega en la práctica en una doble dimensión. De un lado, imponiendo a los poderes públicos el mandato de publicar todas las informaciones que sean relevantes para conocer y fiscalizar sus actuaciones (lo que se conoce como *publicidad activa*). Y, de otro lado, garantizando a todas las personas sin distinción el derecho a acceder directamente a los contenidos y a los documentos que obren en poder de las administraciones públicas y demás sujetos obligados (el *derecho de acceso a la información pública*).

Con la acción conjunta de estos dos vectores, la transparencia efectiva vigoriza la democracia en la medida en que posibilita que los ciudadanos estén más y mejor informados para participar activamente en la vida pública y, al mismo tiempo, les permite fiscalizar de una manera mucho más eficaz la actuación de los responsables públicos, ya sea a título individual o colectivo. Todo ello redunda en un mayor acercamiento de las administraciones a la ciudadanía y en el fortalecimiento de un valor esencial para la cohesión y el buen funcionamiento de las comunidades

políticas del que hoy en día no andamos muy sobrados: la confianza en las instituciones.

En España hemos acumulado un gran retraso en este campo en comparación con los países de nuestro entorno. Durante mucho tiempo nos hemos limitado a enfoques fragmentarios, estableciendo determinadas obligaciones de publicidad de los actos de los poderes públicos y reconociendo el derecho de acceso la información únicamente en algunos ámbitos específicos. Como consecuencia de ello, carecíamos de una regulación general de las obligaciones de transparencia de los poderes públicos, y adolecíamos también del reconocimiento de un derecho subjetivo, ejercitable por cualquier persona, para acceder a la información en posesión de los organismos y las entidades públicas sin necesidad de acreditar un interés específico.

Estas importantes lagunas no se colmaron hasta el mes de diciembre del año 2013 con la aprobación de la LTAIBG, aunque todavía habría que esperar otro año más para que comenzase a desplegar sus efectos, ya que la propia Ley articuló en su Disposición final primera una entrada en vigor escalonada en tres tiempos, de suerte que solo el título segundo (consagrado al buen gobierno) entró en vigor al día siguiente de su publicación en el BOE, mientras que la eficacia de los títulos preliminar, primero y tercero (dedicados al objeto, la transparencia de la actividad pública y al Consejo de Transparencia y Buen Gobierno, respectivamente) se pospuso al momento de cumplir un año de la publicación; y, por otra parte, a las Comunidades Autónomas y a las Entidades Locales se les concedió un plazo máximo de dos años para adaptarse a las obligaciones contenidas en la Ley.

Estando pues a punto de cumplirse diez años desde la aprobación de la LTAIBG, y cuando nos acercamos a los nueve de vigencia efectiva (ocho en el caso de las Comunidades Autónomas y las Entidades Locales), es un buen momento para hacer balance, para computar los progresos, analizar las fallas, y alistar las tareas pendientes.

Hoy en día nadie discute que la LTAIBG ha contribuido decisivamente al rápido desarrollo de la transparencia pública en nuestro país, no sólo por su específico contenido normativo y su impacto directo en el ámbito de la Administración General del Estado sino también porque operó como detonante, generando una muy fructífera dinámica que ha logrado transformar notablemente el panorama de la transparencia y del derecho de acceso a la información pública en todos los niveles del Estado español. Prácticamente todas las Comunidades Autónomas han aprobado sus leyes de transparencia y muchas de ellas han creado sus propios órganos de garantía. Hay también cuantiosa normativa adoptada por las Entidades Locales, y desde la Federación Española de Municipios y Provincias se está llevando a cabo una vigorosa labor de impulso y consolidación. En términos generales, todas las administraciones han realizado un encomiable esfuerzo en sus respectivos

ámbitos para poner en marcha portales de transparencia, crear unidades especializadas e ir incorporando la cultura de la trasparencia a su funcionamiento diario.

A esta transformación han coadyuvado en gran medida los órganos garantes de la transparencia y del derecho de acceso a la información pública, los Consejos y los Comisionados de Transparencia que, desde el momento mismo de su creación, a pesar de los escasos medios disponibles, se han empleado a fondo en el objetivo compartido de superar el retraso acumulado y avanzar hacia la consolidación de la transparencia como un auténtico principio rector de la vida pública en nuestro país. Con este fin, vienen tutelando el derecho de acceso a la información pública con firmeza y rigor jurídico, construyendo un valioso acervo interpretativo que proporciona, tanto a la ciudadanía como a los sujetos obligados, un notable grado de certeza sobre el contenido y alcance del derecho y que, cuando ha sido cuestionado judicialmente, en la gran mayoría de los casos obtuvo el respaldo de nuestros Tribunales de Justicia. En paralelo, muchos de ellos llevan a cabo además una compleja tarea de evaluación periódica del grado de observancia de las obligaciones legales que, aparte de su función estricta de control, está mostrando una gran eficacia incentivadora del cumplimiento.

No obstante, es obligado precisar que el gran avance conseguido en este campo en menos de una década no es solo el resultado de la actuación de las administraciones y de los órganos de garantía sino el fruto de una gran labor colectiva en la que han participado múltiples actores: junto a funcionarios y empleados públicos, también organizaciones sociales y políticas, jueces y magistrados, académicos, periodistas, archiveros, documentalistas, y otros muchos colectivos y profesionales.

Ahora bien, siendo muy notables los avances conseguidos estos años, no cabe desconocer que aún queda un considerable trecho por recorrer para que el mandato con el que arranca el preámbulo de la LTAIBG, que prescribe que «[l]*a transparencia, el acceso a la información pública y las normas de buen gobierno deben ser los ejes fundamentales de toda acción política*», se haga plena realidad en nuestro país, situándolo así en el lugar que le debería corresponder en el contexto internacional. Para continuar progresando hacia ese ambicionado nivel de transparencia necesitamos, como ya he reclamado en otras ocasiones, actuaciones decididas, tanto en el ámbito de las políticas públicas como en plano normativo.

Es necesario que todas las administraciones refuercen sus políticas de transparencia y elaboren planes generales y específicos en la materia (con sus correspondientes sistemas de seguimiento y evaluación), determinando los objetivos, los procedimientos, las medidas y las respectivas responsabilidades, con el fin cumplir adecuadamente con las obligaciones de publicidad activa y atender correctamente las solicitudes de acceso a la información pública. También resulta urgente mejorar la dotación de medios, tanto de los órganos de garantía -que en su mayoría

continúan sufriendo una situación de precariedad, sin los recursos personales y materiales necesarios-, como de las unidades de transparencia, a las que corresponde un importantísimo papel en el buen funcionamiento del sistema y cuyo escaso personal ha de simultanear muchas veces las tareas de transparencia con otras igualmente exigentes como la de atención a la ciudadanía o la protección de datos personales.

Y, en todo caso, son indispensables reformas legislativas, particularmente en lo que concierne a la LTAIBG, que ya nació con algunas carencias y ciertos defectos de técnica legislativa que, con el paso del tiempo y la experiencia adquirida con su aplicación, se han ido haciendo más evidentes y hoy nadie duda que están frenando el avance hacia la implantación efectiva del principio de transparencia en nuestro país. Lógicamente, no es este el lugar para analizar y exponer con el debido detalle los diversos aspectos necesitados de reforma, pero no puedo menos que enunciar, aunque sea telegráficamente, algunos de los más relevantes. Así, aparte del reconocimiento de la naturaleza iusfundamental del derecho de acceso a la información pública, la garantía de su eficacia práctica requiere el fortalecimiento institucional del Consejo de Transparencia, atribuyéndole las potestades necesarias para ejercer con plenitud sus funciones de supervisión y control, comenzando por las de carácter coercitivo para reaccionar frente a la negativa de los sujetos obligados a cumplir con sus resoluciones o el retraso en ejecutarlas. El ámbito subjetivo de aplicación, los procedimientos de acceso y de reclamación, la articulación del régimen general de acceso a la información pública con los regímenes específicos o el alcance de la cláusula de supletoriedad son también, entre otros, aspectos de la ley necesitados de revisión y clarificación.

Junto a las políticas públicas y las reformas legislativas, para que el principio de trasparencia alcance plena eficacia, desplegando toda su potencialidad, son igualmente indispensables buenos estudios doctrinales, que analicen en profundidad los múltiples problemas que su implementación suscita en las complejas sociedades actuales; estudios que, a la vez, ofrezcan a los aplicadores pautas y propuestas sólidamente articuladas que permitan ir construyendo día a día las mejores respuestas para garantizar la coexistencia equilibrada de la transparencia pública con los derechos individuales y el buen funcionamiento del sistema democrático en un contexto en el que la acelerada evolución tecnológica genera de continuo arduos retos.

Los estudios que integran este monográfico responden claramente a los objetivos enunciados al abordar cuestiones nucleares como los conflictos entre transparencia y protección de datos, la transparencia como garantía de la integridad de los procesos electorales en entornos digitales, la transparencia algorítmica en medios de comunicación, plataformas y servicios digitales, las obligaciones de transparencia de las autoridades de control, la protección de las personas informantes, o el potencial del *data mining* en la lucha contra la corrupción; y, todo ello, contemplando

no solo el derecho nacional sino prestando especial atención a los desarrollos habidos en el seno la Unión Europea y, muy en particular, a los proyectos en gestación y sus potenciales efectos sobre el ordenamiento español.

En conjunto, este monográfico contiene un rico mosaico de análisis, reflexiones y propuestas que, desde enfoques diversos y complementarios, arrojan luces muy clarificadoras sobre la poliédrica realidad de la transparencia pública cuya proyección práctica plantea aún no pocos interrogantes. Animo por tanto a todos los interesados en el tema a adentrarse en la lectura de estos textos con la convicción de que no se verán defraudados, pues la trayectoria académica y profesional de sus autores otorga la máxima garantía de calidad.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

Transparencia, un derecho europeo, y su relación con otros bienes constitucionalmente relevantes

Juan F. López Aguilar[1]

Catedrático de Derecho Constitucional

Universidad de Las Palmas de Gran Canaria

España

ORCID : 0000-0002-6564-2536

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

RESUMEN: Este artículo analiza el derecho a la transparencia en el marco del Derecho europeo y su relación con los derechos de privacidad y protección de datos. Se examinan las regulaciones existentes y su papel en la promoción de la rendición de cuentas, mientras que se destaca la importancia de equilibrar la protección de la privacidad y la transparencia institucional. Además, se profundiza en el debate sobre la transparencia y el acceso a la información en el Derecho europeo, así como la relevancia de la jurisprudencia del Tribunal de Justicia de la Unión Europea.

PALABRAS CLAVE: protección de datos, transparencia, derecho europeo, privacidad.

CONTENIDOS: 1.-Introducción. 2.-El encuadramiento del derecho a la transparencia y su regulación en el Derecho europeo. 3.-Los derechos de la privacidad y de protección de datos en su relación dialéctica o conflictiva con los derechos a la transparencia y acceso a la información en el Derecho europeo. 4.-Los desarrollos más recientes del debate alrededor de la transparencia y el acceso a la información en el Derecho europeo. 5.-La relevancia del "Case Law": la jurisprudencia del TJUE. 6.-Particular referencia a los derechos a la transparencia y acceso a la información en el marco de la lucha contra la corrupción y el blanqueo. 7.-Consideraciones conclusivas. -Bibliografía.

[1] Catedrático de Derecho Constitucional (ULPGC). Presidente de la Comisión de Libertades, Justicia e Interior del Parlamento Europeo.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

Transparency, a European right, and its relationship with other constitutionally relevant goods

ABSTRACT: This article analyses the right to transparency under European law and its connexion with the rights to privacy and data protection. It examines existing regulations and their role in promoting accountability, while highlighting the importance of balancing privacy protection and institutional transparency. In addition, it delves into the debate on transparency and access to information in European law, as well as the relevance of the case law of the Court of Justice of the European Union.

KEYWORDS: data protection, transparency, european law/ privacy.

1.- Introducción

El concepto jurídico de *transparencia* responde a una construcción aún reciente en la historia del Derecho de la UE. Se trata pues de un inequívoco avance en el ordenamiento europeo, concretamente encuadrado en la configuración de los *derechos de última generación* (arts.41 y 42 de la *Carta de Derechos Fundamentales de la UE*, CDFUE), así llamados por incardinarse en los desarrollos más recientes de la configuración jurídica de los derechos fundamentales (como ejemplifican también la cláusula de no discriminación de su art.21, la prohibición de prácticas eugenésicas, del lucro con órganos humanos y de la clonación de su art.3, o la consagración expresa del consentimiento y de los derechos de acceso y de rectificación en la protección de datos, garantizada en todo caso por una Autoridad independiente, en su art.8).

Este novedoso *derecho a la transparencia* aparece vinculado en su raíz al derecho de *acceso a la documentación* obrante en poder de los poderes públicos y de las administraciones, y a su correlativo derecho al "*buen gobierno*" o la gobernanza de calidad (articulado, hasta la fecha, en el Reglamento 1049/2001, de acceso del público a los documentos del PE; del Consejo y de la Comisión)[2].

En el constitucionalismo comparado europeo es frecuente encontrar cláusulas generales reconocedoras de derechos de participación y acceso a la actividad de la administración, acceso de los interesados al procedimiento administrativo que les

[2] Cfr., por todos, los trabajos especializados al respecto de GUICHOT (2023), y la bibliografía relevante allí citada.

CC BY SA

DOI: https://doi.org/10.51915/ret.305

afecte, audiencia de los de los ciudadanos y derecho a ser informado de la actuación administrativa y de la elaboración de las disposiciones y actos, con base en el interés general o en el interés específico de personas o colectivos concernidos (véase, por ejemplo, arts.23, 103 y 105 de la Constitución española de 1978, CE). Todo ello en el cuadro del imperio de la ley y de la sujeción de toda la actividad de la Administración al principio de legalidad, en todo caso susceptible de control jurisdiccional (véanse así los arts.9.1 y 106 CE).

En el constitucionalismo escrito más avanzado en nuestro entorno pueden encontrarse además disposiciones específicas previendo la conjugación de los derechos de acceso y de participación con otros bienes constitucionalmente relevantes, como la seguridad del Estado, la preservación de la independencia judicial en la investigación de los delitos (así, el tradicionalmente llamado "secreto del sumario" en España) y, con relieve especial, la esfera de la intimidad y/o privacidad sobre la que se cimienta el derecho a la confidencialidad de los datos y de las comunicaciones personales y a la protección de datos.

En cuanto a su encuadre europeo, motor de su prefiguración jurídica y de su remarcable avance, nada puede entenderse sin ponderar la medida e impacto, ciertamente decisivo, de la entrada en vigor (diciembre de 2009) del *Tratado de Lisboa* (TL) y de la CDFUE, revestida del "mismo valor jurídico que los Tratados" (art.6.1 TUE). Sobre el proceso de construcción europea he publicado en los últimos años varias monografías y artículos especializados. En ellos he examinado, con la extensión que merece, el impacto de la crisis que arrancó en 2008 -a la que solemos referirnos como la *Gran Recesión*- sobre el conjunto de la UE y sus Estados miembros (EEMM), afectando a sus *valores comunes* (art.2 TUE) y a la propia *voluntad de Europa*. Se acentuó así un contraste -ampliamente debatido en tribunas de opinión y en la literatura académica- entre objetivos proclamados desde la entrada en vigor del TL en 2009, y sus realizaciones.

Este entorno turbulento, sujeto a inestabilidades e intensas vicisitudes en los paisajes políticos de los EEMM y en la composición del propio Parlamento Europeo (PE), alcanzó inevitablemente al despliegue del ambicioso programa político y legislativo que se condensa en el *Espacio de Libertad, Justicia y Seguridad* (ELSJ, Título V TFUE, arts. 67 a 89), cuyas disposiciones deben además leerse e interpretarse conforme a la CDFUE[3].Y esta aseveración requiere de alguna ilustración adicional en este apartado introductorio, puesto que lo que nos proponemos como objeto de estas páginas es revisar el trayecto y el actual estadio de desarrollo de una relación dialéctica entre derechos fundamentales consagrados en la CDFUE (de un lado, la privacidad y la protección de datos de sus arts.7 y 8; de otro, los de la transparencia

[3] Ver DI FEDERICO (2011).

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

y acceso a la información, arts.41 y 42) y de su tratamiento desde el Derecho europeo legislado por el PE:

He sostenido en mis anteriores publicaciones un principio relevante del que estoy profundamente convencido: en la experiencia de integración supranacional europea, fundada y regida por el Derecho, la CDFUE es -a mi juicio, junto al ELSJ- la expresión más completa, hasta el momento presente, de su dimensión política y ambición constitucional[4]. La CDFUE, revestida del "mismo valor jurídico que los Tratados" (art. 6.2 TUE), consagra un conjunto de derechos de *última generación* junto a los que clásicamente vertebran los capítulos dogmáticos (derechos y libertades, junto a principios rectores, capítulos II y III del Título I CE) de las Constituciones nacionales de los EEMM. Entre otros derechos novedosos (así, los incardinados en la "autodeterminación informativa" ante la revolución tecnológica y la sociedad digital; los derechos vinculados a la dignidad personal ante los avances de la genética y la investigación sobre el genoma humano), la CDFUE consagra derechos específicos vinculados al principio del "derecho al buen gobierno" y "buena administración", en combinación con el principio de "apertura" y "transparencia" (arts. 41 y 42 CDFUE). Y sobresale, especialmente, el derecho de "*acceso* a la documentación en poder de la Administración, y el derecho a la "*transparencia*" y al escrutinio público sobre actos y decisiones de los poderes públicos.

2.- El encuadramiento del derecho a la transparencia y su regulación en el Derecho europeo

El ahora así denominado *derecho a la transparencia* ("*Openness" y "Transparency*") reconfigura otros derechos que con anterioridad venían reconocidos en los ordenamientos de los EEMM (así, en España, art. 105 CE, y las leyes: *Ley 30/92 LRJ-PAC*[5]; *Ley 19/2013 de Transparencia*[6], y las posteriores leyes aprobadas en 2015, del *Procedimiento Administrativo Común*[7] y del *Régimen Jurídico del Sector Público*[8]).

Transcurrida holgadamente más de una década desde la entrada en vigor del TL y la CDFUE, el acervo europeo cuenta ya con un corpus conformado por los correspondientes actos legislativos, las Resoluciones e Informes del PE y la jurisprudencia del TJUE como órgano de garantía de la primacía del Derecho

[4] LÓPEZ AGUILAR (2017 a); Cfr. MUÑOZ MACHADO (2017: 195-230).

[5] Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

[6] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

[7] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

[8] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

europeo, de su eficacia directa (y de su efecto útil) y de su interpretación uniforme (arts. 19 TUE y 251 a 267 TFUE).

El paisaje resultante es, sin embargo, a estas alturas, incompleto y por tanto todavía insatisfactorio. Influyen en ese balance el progresivo desfallecimiento de la confianza mutua y del reconocimiento mutuo en la cooperación judicial: a título de elocuente ejemplo, los debates alrededor del alcance y operatividad de la *Orden Europea de Arresto*, Decisión Marco de 2002, conocida *Euroorden*, ilustra el comentado contraste entre objetivos y resultados[9]. Esta problemática se acentúa al señalarse al Consejo -en su función legislativa, colegislador europeo con el PE - como eslabón crecientemente disfuncional del *Decision Making* europeo, propenso a una *regresión nacional* de las bases jurídicas europeas, en una tendencia que resulta difícilmente conciliable con el denominado método comunitario[10]. Así, el balance final de la Legislatura europea 2014-2019 mostró con claridad preocupante el alto número de ocasiones en que el Consejo bloqueó -por falta de voluntad para alcanzar las preceptivas "mayorías cualificadas" so pretexto de un "consenso" que encubre unanimidades más allá de lo exigible- una parte sustancial de la legislación previamente aprobada e impulsada desde el PE. Innumerables veces se prolongaron los *trílogos* hasta el agotamiento de los procedimientos legislativos en curso, sin que llegasen a alcanzar su aprobación definitiva, a costa de erosionar a la confianza de la ciudadanía en la capacidad de respuesta de la arquitectura europea frente a desafíos sumatorios y en la credibilidad misma de las Instituciones[11].

De esa "glaciación europea" -desfallecimiento de la requerible voluntad de Europa- he escrito con mayor detalle en mi libro *Europa, Parlamento, Derechos: Paisaje tras la Gran Recesión*, 2017. Explico en su texto hasta qué punto muchas iniciativas adoptadas en su día por la Comisión Europea y discutidas y votadas (con mayorías favorables de geometría variable) en el PE, sufrieron después su estancamiento o bloqueo sistemático por parte del Consejo[12]. Lo que sin duda resulta particularmente nocivo en su alcance sobre el despliegue de las potencialidades del Título V del TFUE (arts.67 a 89) que establece el ELSJ. Y ello porque éste incorpora, como subrayé anteriormente, la comprensión más acabada de la dimensión política (y constitucional) de la integración supranacional europea.

Lo hace no sólo al ensanchar cualitativamente el *ámbito material* de las competencias de la UE (al menos 80 políticas de nuevo cuño) sino al hacer del PE,

[9] Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros.

[10] Véase LÓPEZ AGUILAR (2013).

[11] Ver, con carácter general, GARZÓN GLARIANA (2015: 43-83) y mi último libro al respecto, LÓPEZ AGUILAR (2020).

[12] Cfr. ABRISKETA URIARTE (2017: 119-158).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

en ese amplio arco de materias, *legislador europeo "en pie de igualdad" con el Consejo*, lo que, por cierto, lo realza como el *único Parlamento* del mundo directamente electivo, democráticamente legitimado, es supranacional en su alcance y revestido de potestad legislativa y presupuestaria, tal como he explicado en mi libro *El Parlamento Europeo: una experiencia única***,** Wolters Kluwers, 2020. Y lo hace también, sobre todo, al asumir para el PE poderes legislativos sobre materias tradicionalmente consideradas como *regalía* del Estado, esto es, como tradicional reserva de soberanía de los EEMM: ese es, notoriamente, el caso de la legislación sobre derechos fundamentales, de la legislación penal y de garantías procesales y de la cooperación policial y judicial sobre los fundamentos de la "confianza mutua" y el "reconocimiento mutuo" de resoluciones jurisdiccionales, postulados estos basados en la consagración de unos "*valores comunes*" (art.2 TUE), y unos principios generales y tradiciones constitucionales comunes que cimientan una *idea europea*, tan distintiva como netamente europea, del *Estado de Derecho, la democracia y los derechos fundamentales*.

Este y no otro es el pilar del actualmente vigente *Rule of Law, Democracy and Fundamental Rights Framework* y *Policy Cycle*, que apoyan el *Annual Report* y los 27 *Country Reports* que, de forma regular, periódica y sobre parámetros objetivados, presenta la Comisión Europea (Comisario de Justicia). Y este y no otro es el marco en el que cobran sentido tanto el procedimiento de sanción extraordinaria ante situaciones de "riesgo cierto" (*Clear Risk*) de "violación grave y sistémica" de dichos valores comunes (*Serious Breach*) contemplado en el art.7.2 TUE, así como el *Reglamento de Condicionalidad del acceso a los Fondos UE respecto del cumplimiento del Estado de Derecho* (*Rule of Law Conditionality Regulation, 2020/2092*) vigente desde 2021.

Estas, entre otras materias, hacen de la *Comisión de Libertades, Justicia e Interior del PE* (Comisión LIBE, en la jerga) la de mayor competencia legislativa, extendiendo su amplio radio sobre un círculo que va desde los derechos fundamentales (con su régimen de aplicación delineado en los arts.51 a 54 CDFUE) a la seguridad interior, pasando por la gestión integrada de fronteras exteriores y libre circulación (*Espacio Schengen*), migraciones y asilo, Derecho penal y procesal y cooperación judicial. Por lo que la Comisión LIBE del PE es la Comisión competente para regular el derecho a la transparencia y acceso a la información en el Derecho europeo, y para asegurar su compatibilidad con el estándar europeo de privacidad y protección de datos, sin duda el más alto del mundo.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

3.- Los derechos de la privacidad y de protección de datos en su relación dialéctica o conflictiva con los derechos a la transparencia y acceso a la información en el Derecho europeo

Pues bien, desde estas consideraciones, cabe afirmar con claridad que la protección de la privacidad y los datos personales vertebra seguramente, bajo la cobertura de la cláusula del "respeto la vida privada" (privacidad e intimidad, personal y familiar), uno de los más distintivos activos del Derecho europeo, estableciendo el que, a mi juicio, es el estándar de garantía del derecho fundamental más alto e intenso del mundo, que sin duda alguna incide en el alcance práctico del derecho a la transparencia y acceso a la información[13].

Obsérvese, a este respecto, que los derechos de la transparencia y de la privacidad revisten ambos, en la CDFUE, rango de derechos fundamentales de la ciudadanía europea, mientras que en las Constituciones nacionales de los EEMM (así por ejemplo la CE, arts.105 y 18.4), la cualificación de cada derecho se corresponde, variadamente, con cada específico régimen de protección protegido. Acerca de la interacción de ambas categorías de derechos ("enfrentados", "conjugados", mutuamente interactivos) la doctrina especializada ha desarrollado a fondo el test de su ponderación ("caso por caso", legitimidad de su finalidad o principio de fin legítimo, y criterios de razonabilidad y proporcionalidad), así como los denominados "derechos de oposición" por los "intereses en juego" (interés general; datos especialmente protegidos; otras situaciones especiales, como, notablemente, datos relativos a menores de edad y a la seguridad de personas vulnerables).

También en trabajos anteriores he examinado con detalle el *iter* legislativo que condujo a la aprobación -en la Legislatura 2009/2014 del PE, en cuyo arranque entró en vigor el TL junto con la CDFUE-, del actualmente vigente *Data Protection Package* (Reglamento general, GDPR, 679/2016; y Directiva de *Law Enforcement*, 680/2016, actos legislativos ambos plenamente vinculantes para los EEMM y para los actores privados desde 2018), cuyo procedimiento legislativo recayó en las competencias de la Comisión LIBE[14]. Correlativamente, me he ocupado también de los concretos problemas suscitados por este elevado nivel europeo de protección en el régimen jurídico de transmisión de datos con países terceros y organizaciones internacionales, lo que es especialmente notable en la *relación transatlántica* entre la UE y los EEUU, toda vez que dos sentencias importantes del TJUE (*Schrems I*, C-

[13] Cfr. ANTONINO DE LA CÁMARA (2017: 1-20).

[14] Entre otros avances significativos, el *Data Protection Package* introdujo el "derecho al olvido" (*Right fo be Forgotten*) reforzando los principios de consentimiento expreso y de transparencia; el robustecimiento de los derechos de acceso, rectificación y cancelación del titular de los datos personales; la llamada "data portability" en "*data protection by design and by default*", junto al endurecimiento del régimen sancionador.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.305

362/14 2015:650; y *Schrems II*, C-311/18, 2020:559) anularon las respectivas "decisiones de adecuación" (*Adequacy Decisions*) adoptadas por la Comisión Europea sobre la base, respectivamente, de los entonces vigentes "*Safe Harbor Agreement*" y "*Privacy Shield*" como marco de cobertura para la transmisión a EEUU de datos personales de los europeos[15].

En este concreto contexto merece mención especial la Resolución adoptada por la Comisión LIBE acerca de la "adecuación" de la protección de datos de la ciudadanía europea en el futurible nuevo marco (actualmente en curso de negociación) del *EU/US Data Privacy Framework*. El punto más relevante es que la mayoría (*Rapporteur & Shadow Rapporteurs*) ha decidido denegar su apoyo a la *Adequacy Decision* que debe adoptar la Comisión Europea. La posición de la Comisión LIBE parte de que la privacidad y la protección de datos son, efectivamente, derechos fundamentales directamente invocables tanto conforme a la CDFUE como a la jurisprudencia del TJUE vinculante para los poderes judiciales de los EEMM. La objeción determinante descansa en la insuficiencia de los recursos judiciales ejercitables por los ciudadanos europeos ante el sistema judicial de EEUU, particularmente a la luz de las actividades de inteligencia (*US National Security Agency*). Aun siendo conscientes de que este es el tercer intento por parte de la Comisión Europea de subvenir al soporte jurídico de la transferencia de datos en la relación transatlántica UE/EEUU, lo cierto es que la decisión en manos de la Comisión Europea continúa descansando en una *Executive Order* (14086, "*On Enhancing Safeguards for US Signals Intelligence Activities*) dictada por el Presidente Joe Biden, que sin embargo puede ser enteramente revocada por el mismo o cualquier otro Presidente en cualquier momento.

Ciertamente, la *Orden Ejecutiva* del Presidente Biden contempla algunas garantías entre otros avances estimables, incorporando los principios de *"necessity*" y "*proportionality*" (en consonancia con el art.52.1 CDFUE), así como un mecanismo correctivo en caso de violación del *Framework Agreement*. Pero, con todo y con eso, persiste la no correspondencia con los estándares exigidos por el Derecho europeo (GDPR y jurisprudencia del TJUE) para asegurar un "nivel adecuado" de protección, notablemente ante la ausencia de una prohibición expresa de la denominada "*bulk collection of data*" (recopilación masiva e indiscriminada de datos que incluye el contenido mismo de las comunicaciones). En cuanto a los recursos disponibles frente a las infracciones, el régimen de EEUU continúa asentado en el secreto, lo que excluye la obligación de comunicación al titular de los datos y, consiguientemente, los derechos de acceso, rectificación y cancelación consagrados en el art.8 CDFUE. Adicionalmente, la denominada *Data Protection Review Court/* DPRC no forma propiamente parte del Poder Judicial de los EEUU del Art.III de la Constitución de EEUU (sino del Ejecutivo, Art.II), en modo que sus decisiones pueden ser clasificadas

[15] Ver, sobre este punto, LÓPEZ AGUILAR (2017 b): 557-581).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

como materia reservada. La representación del interesado (titular de los datos) se confía a un "*Special Advocate*" designado por la DPRC sin garantías de independencia ni posibilidad de recurso a Tribunales federales (lo que contraviene el estándar del art.47 CDFUE acerca de la "imparcialidad" e "independencia" judicial). Finalmente, debe además tenerse en cuenta que, a diferencia del modelo europeo (con legislación europea sobre protección de datos), no existe todavía en EEUU una Ley federal de protección de datos. Dicho todo lo cual, debe notarse, sin embargo, que hasta el momento presente (en la redacción de estas líneas), la Comisión Europea se muestra confiada en el resultado final de su negociación superará el examen del TJUE asentado en los casos precedentes de *Schrems I* (2015) y *Schrems II* (2020); en otras palabras: "*There will be no Schrems III CJEU Case*".

Visto todo lo anterior, en el cuadro de los instrumentos disponibles en el Derecho europeo debe todavía complementarse con una serie de actos legislativos sectoriales, entre los que destacan la Directiva 681/2016, sobre utilización de datos del *Registro de Nombres de los Pasajeros* (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y delincuencia grave; el capítulo VI (garantías en materia de protección de datos) del Reglamento 2016/794, relativo a la *Agencia UE de Cooperación Policial* (Europol); el capítulo VIII (protección de datos) del Reglamento 2017/1939 por el que se establece por cooperación reforzada la Fiscalía Europea; y acuerdos internacionales sobre transferencia de datos en base al art.45 GDPR (decisión por la Comisión Europea de la estimación de un "nivel adecuado de protección de datos" por parte de un país tercero, llamada *Adequacy Decision*), como ejemplifican el *Acuerdo Marco* UE/EEUU de protección de datos sobre la prevención, investigación, detección y enjuiciamiento de infracciones penales en la lucha contra el terrorismo y el crimen organizado, así como los Acuerdos UE/EEUU, UE/Australia y UE/Canadá de datos PN, y el *Programa UE/EEUU de Seguimiento de la Financiación del Terrorismo*.

Además de todo ello, el PE ha adoptado un abultado número de Resoluciones sobre protección de datos y de la privacidad en ámbitos específicos, tras otros tantos debates en Comisión LIBE y en Pleno, así como mantenido interlocución regular con la Autoridad Europea de Protección de Datos (EDPS, institución independiente de supervisión del cumplimiento de la legislación vigente por la UE, sus Instituciones y sus EEMM) y con el Comité Europeo de Protección de Datos (EDPB, sucesor del antiguo *Art.29 Working Party,* en referencia a la derogada Directiva 45/2001), con amplios poderes para la resolución de litigios entre las autoridades nacionales de supervisión y para asesorar y orientar acerca de elementos clave del GDPR y de la Directiva de Protección de Datos en el ámbito penal (*Law Enforcement Directive*).

El rango fundamental de estos actos normativos se corresponde con su alcance general y su importancia material. Lo ejemplifica que en España esta normativa europea haya dado lugar al primer supuesto histórico de desplazamiento de una ley orgánica (la LO 15/99, de 15 octubre, entonces vigente), en la medida en que afecta

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

al desarrollo de derechos fundamentales consagrados en la Constitución española/CE 1978 (art.18.4), habiendo determinado, por consiguiente, la aprobación de la actualmente vigente nueva Ley española de Protección de Datos (LO 2/2018, de 5 de noviembre), consistente con las exigencias del nuevo marco europeo establecido en el GDPR[16].

No es extraño, por lo tanto, que éste sea seguramente el punto más elaborado en la doctrina jurídica del muy contemporáneo régimen jurídico de la transparencia y acceso a la información y a los documentos públicos: el de su ponderación con la protección de datos y la privacidad. La matriz de este ensamblaje de derechos es netamente europea. El primer círculo concéntrico de referencia lo presta, como es conocido, el ordenamiento del Consejo de Europa (CdE), cuyo fruto más granado es el *Convenio Europeo de Derechos Humanos* de 1950 y sucesivos Protocolos bajo la garantía jurisdiccional del TEDH (art.8 CEDH; Convenio CdE 108/81 sobre protección de datos y Convenio CdE 205/2009 sobre acceso a los documentos públicos)[17].

En el segundo círculo concéntrico, el del Derecho de la UE (art.16 TFUE), la *Carta Europea de Derechos Fundamentales de la UE*/CDFUE consagra derechos fundamentales cruciales en éste ámbito: arts. 7, 8, 10, 41y 42, El desarrollo del principio relativo a la transparencia lo ofrece, hasta la fecha, un instrumento normativo previo a la entrada en vigor del TL y la CDFUE (2009), el *Reglamento de Transparencia y Acceso a los Documentos Públicos* de 1049/2001 (todavía hoy pendiente, más de 20 años después, de actualización impulsada desde el PE y bloqueada por el Consejo), iluminado, ciertamente, por la sobrevenida CDFUE (arts.41 y 42) y por la jurisprudencia interpretativa del TJUE (vinculante, en su función de garante del "respeto del Derecho", art.19 TUE), en la que sobresalen los casos *Capitani I* (sentencia del Tribunal General de 22 de marzo de 2018) y *Capitani II* (sentencia del Tribunal General de 25 de enero de 2023). De acuerdo con la jurisprudencia interpretativa el TJUE, los límites a la transparencia aparecen vinculados al estándar europeo de protección de datos en tres ámbitos correlacionados en un gradiente de intensidad decreciente: a)- información pública en la que se contengan datos personales especialmente protegidos; b)- información pública que afecte, con carácter general, a datos personales; c)- información que contenga datos "meramente identificativos".

La transposición española de este específico segmento del Derecho de la UE es la que ofrece la actualmente vigente Ley 19/2013 de 9 de diciembre, de *Transparencia, Acceso a la Información Pública y Buen Gobierno*, con su desarrollo reglamentario (instituyendo el Consejo de Transparencia y Buen Gobierno, al que se encomienda la supervisión de su cumplimiento) y sus leyes complementarias (Ley 37/2007, de

[16] Cfr. GARCÍA MAHAMUT, R. (2019: 95-132).

[17] Véase, por todos, CERRILLO I MARTÍNEZ (2017: 127-156).

DOI: https://doi.org/10.51915/ret.305

16 de noviembre, *de Reutilización de Información en el Sector Público*), acompañada, como no podía ser de otra manera, de una interesante casuística de supuestos de conflicto entre el derecho a la transparencia y el de protección de datos entre otros relativos a la garantía constitucional de la intimidad personal y familiar, concreción española del derecho comparado a la privacidad (datos relativos a la ideología, a la afiliación sindical, religión, creencias; origen racial, salud, vida sexual; registro de infracciones penales o administrativas).

Figuran en la Ley española, junto a estos derechos fundamentales, otros bienes jurídicos relevantes y complementarios como la seguridad nacional, la defensa y las relaciones exteriores; la seguridad pública; la prevención, investigación y represión de los delitos e ilícitos penales, administrativos o disciplinarios; la igualdad de armas procesal y la tutela judicial efectiva; las funciones administrativas de vigilancia, inspección y control; los intereses económicos y comerciales; la política económica monetaria; el secreto profesional y la propiedad intelectual e industrial: la garantía de la confidencialidad y el secreto constitucional o legalmente protegido; la tutela del medio ambiente.

De acuerdo con la legislación española, las Administraciones públicas no tienen potestad discrecional para denegar el acceso a la información pública, debiendo cualquier decisión limitativa acreditarse debidamente motivada. Ni siquiera la concurrencia de una base legal, derecho subjetivo o interés legítimo para la invocación de un límite equivale mecánicamente a la denegación del acceso a la información pública, debiendo razonarse, en contrario, un perjuicio concreto, definido y evaluable, pudiendo determinarse mediante los denominados "test del daño concreto" y "test de la ponderación de intereses" (con resultado, en su caso, de "acceso parcial" o "limitado" con fundamentación sujeta al complementario "test de razonabilidad y proporcionalidad").

4.- Los desarrollos más recientes del debate alrededor de la transparencia y el acceso a la información en el Derecho europeo

Hasta aquí la referencia, argumentalmente obligada, al contexto en el que cabe encuadrar históricamente la iniciativa de *Transparencia y Acceso a los Documentos de las Instituciones*, adoptada por la Comisión y debatida extensamente durante la Legislatura 2009-2014 del PE, en la que asumí la Presidencia de la Comisión de Libertades, Justicia y Asuntos de Interior (LIBE) (con seguridad la de mayor carga legislativa de trabajo y más intensiva agenda de reuniones y votos).

Partamos en este apartado de la secuencia descrita en cuanto a la evolución del ordenamiento europeo desde la entrada en vigor del TL y la CDFUE. No es difícil calibrar la desazón que suscitan las dificultades surgidas para la actualización del ELSJ (pendiente, en la Legislatura 2019/2024, de la finalización del debate legislativo a propósito de la *Schengen Governance Act* y del *New Migration & Asylum Pact*, compuesto por cinco Reglamentos, que deberían haber completado a estas alturas

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

un espacio europeo de libre circulación de personas y un *Sistema Europeo Común de Asilo* basado en la responsabilidad compartida y la solidaridad tal y como mandata el art. 80 TFUE. Es innegable, sin embargo, que, antes bien de haberse completado el programa contenido en el ELSJ, éste se ha visto sometido a los sucesivos embates de una tendencia regresiva (si es que no degradante, *watering down effect*) del acervo vigente, teñida de un distorsionante sesgo *seguritario* en el control de las fronteras frente al hecho migratorio (visto como una amenaza por una parte sustancial de los miembros del Consejo) y por el reforzamiento de los instrumentos de retorno de migrantes irregulares ("*not eligible to stay*") UE[18].

En lo que nos interesa al objeto de estas páginas, este debate se conecta con la interoperabilidad (*Interoperability Package*) del llamado "*Sistema de Información de Visados*"[19] de última generación (*VIS II*), en combinación con el llamado *Sistema de Información Schengen II*[20], junto al *Sistema de Entradas y Salidas*[21] coordinadas por *EU-Lisa*[22], además de la acepción marcadamente seguritaria (desde una visión que bascula desde la prevención negativa hasta el declarado rechazo) del *Código de*

[18] Sobre el procedimiento legislativo europeo, con carácter general, véase BARON CRESPO (2006).

[19] Reglamento (CE) núm. 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).

[20] Reglamento (CE) núm. 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación («Reglamento SIS II»); y Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación («Decisión SIS II»).

[21] Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) núm. 767/2008 y (UE) núm. 1077/2011; y Reglamento (UE) 2017/2225 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se modifica el Reglamento (UE) 2016/399 en lo que respecta a la utilización del Sistema de Entradas y Salidas.

[22] Reglamento (UE) 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

Fronteras Schengen[23], el *PNR*[24], el Reglamento *Eurodac*[25]. Complementan estas normas otras iniciativas orientadas al "refuerzo" del control de fronteras y, por extensión, al vector de la seguridad en materia de extranjería y asilo y refugio[26], por ende estigmatizados como un "riesgo" para la *Estrategia Interior de Seguridad* en la UE, art. 70 TFUE. El sesgo seguritario[27] ha acabado así impactando sobre el *Decision Making Process*, con consecuencias de calado.

Y es que, efectivamente, el *Open-Decision Making*, con la participación ciudadana, la "*transparencia*" y el derecho "*a la buena administración*" (arts. 41 y 42 CDFUE), apuntalan, por un lado, el fortalecimiento del principio democrático de la sujeción a las reglas del Estado de Derecho (art.2 TUE). Todas las Instituciones de la UE están por lo tanto obligadas por ciertas reglas vinculantes: los arts. 10 y 11 del TUE establecen claramente que "todo ciudadano tiene derecho a participar en la vida democrática de la Unión". Las decisiones serán tomadas de la forma "más abierta y próxima posible a los ciudadanos", en un mandato que conjuga la consagración (art. 101 TUE) de la democracia representativa en el funcionamiento de la UE con un robustecimiento de un complementario vector de democracia participativa. Estas reglas aparecen conectadas, además, con el nuevo mecanismo de *iniciativa ciudadana* (art. 11 TUE), y con la obligación de publicidad vinculante para las instituciones, organismos y agencias de la UE (art. 15 TUE) y con el derecho fundamental de acceso a los documentos (art. 42 CDFUE, que goza, insistimos aquí, del mismo valor jurídico que los Tratados, *ex* art. 6.1 TUE).

Por consiguiente, en la práctica, el principio de "*openness*" y el "*right of access to documents*" se encuentran estrechamente unidos. De modo que el Reglamento todavía hoy vigente (1049/2001), de *Acceso público a los documentos,* descansa

[23] Reglamento por que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de Fronteras Schengen).

[24] Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

[25] Reglamento (UE) núm. 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) núm. 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) núm. 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

[26] Cfr. GARCÍA MAHAMUT y VIGURI CORDERO (2019: 237-270).

[27] Cfr. VIGURI CORDERO (2020).

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

sobre el principio de "acceso más amplio posible", cuyas posibles excepciones (y/o derogaciones, en la jerga comunitaria) deben ser interpretadas con criterio restrictivo. Por su parte, el art. 15.3 TFUE extiende el "derecho de acceso a los documentos" a todas las Instituciones de la UE (pese a que el Reglamento preveía su aplicación inmediata sólo a la Comisión, el Consejo y el Parlamento Europeo), así como a sus organismos y Agencias, si bien tanto el TJUE como los Bancos Central y Banco Europeo de Inversiones sólo se encuentran sujetos a la regla de publicidad en sus procedimientos de carácter administrativo. Por lo demás, son ya varias las Instituciones de la UE que han incorporado en su seno un derecho de acceso análogo al estipulado por el Reglamento 1049/2001.

Han transcurrido más de 20 años desde el vigente Reglamento de 2001, y durante este tiempo han entrado en vigor tanto el TL como la CDFUE. Se comprende fácilmente que en el PE –y muy particularmente en su Comisión LIBE– haya tenido lugar el debate relativo a la demanda (creciente) de su actualización. Vistas las coordenadas hasta aquí expuestas, a lo largo de este tiempo hemos venido asistiendo a la contraposición de dos vectores opuestos: a)- de un lado, el requerimiento de actualización y puesta al día del *acquis* del anterior *Tercer Pilar* ("*Asuntos de Justicia e Interior*") y su conversión al marco dispuesto por el TL ("*lisbonización"*, se la llama): su transposición al nuevo procedimiento legislativo ordinario en que el PE es colegislador en pie de igualdad con el Consejo. b)- de otro, la emergencia creciente y amenazadora de una pulsión antieuropea minada por diversos rebrotes de nacionalismo reaccionario con daños colaterales sobre la consistencia del *modelo social europeo* en multitud de planos[28].

Pues bien, en este contexto, y a pesar de sus dificultades, en el transcurso de la Legislatura europea 2009-2014, primera en la que tuve el honor de presidir cinco años la Comisión de LIBE del PE, recobró fuerza el debate acerca de la pertinencia de actualizar, modificándolo, el vigente *Reglamento de Acceso a los Documentos de la UE* 1049/2001. El Ponente (*Rapporteur*) designado dentro de la Comisión LIBE, el británico Michael Cashman (Grupo S&D), redactó el *Cashman Report on Public Access to European Parliament, Council and Commission Documents* de 2009; complementariamente, por su parte, la eurodiputada sueca (Grupo de los Verdes), Heidi Hautala, fue la Ponente del *Report on Public Access to Documents* correspondiente a 2010-2011. En síntesis, en ambos documentos se asentaron las bases analíticas y los presupuestos críticos para la formulación de una demanda política desde el PE: que la Comisión Europea adoptase una iniciativa legislativa que elevase los estándares de transparencia y acceso a los documentos públicos de todas las instituciones europeas, sus organismos y Agencias, articulando y reforzando los derechos consagrados en los arts. 10 y 11 TUE, art. 15 TFUE y arts. 41 y 42 CDFUE. Pero, con todo y con eso, los trabajos desplegados por la Comisión LIBE

[28] Véase LÓPEZ AGUILAR (2017).

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

–audiencias y comparecencias (*Hearings*), debate y deliberación de una *Own Initiative Report* (art. 225 TFUE), equivalente en el PE a la *Proposición No de Ley* del Derecho Parlamentario español– se vieron finalmente frustrados por la resistencia opuesta por los Gobiernos de los EEMM representados en el Consejo. La Legislatura 2009-2014 concluyó, de esta manera, sin que la versión revisada, actualizada y reforzada del Reglamento 1049/2001 llegase a completar su trámite para ver la luz del día.

Esta secuencia sugiere, en lo cualitativo, un preocupante decalaje entre, por un lado, los objetivos proclamados en el TL y los derechos de ciudadanía consagrados en la CDFUE, y su acusado contraste con, por el otro lado, la capacidad efectiva de las Instituciones decisorias de la UE para asegurar respuestas oportunas a algunos retos planteados. Desde la no correspondencia de la Unión Monetaria e incipiente Unión Bancaria con una (aún muy deficiente) Unión Fiscal europea, hasta la mal llamada "*crisis de los refugiados*" suscitada en 2015 (en realidad una emergencia humanitaria ante la cual el tablero de mandos de la UE entró en *modo de pánico*, imprimiendo desde ahí un *sesgo seguritario* de rechazo refractario frente a los migrantes y demandantes de asilo en todas sus iniciativas internas e internacionales)[29]. Parece obligado colegir que la promesa efectuada desde el TL y la CDFUE se muestra, más de diez años después de su entrada en vigor, todavía un *work in porgress*. Sigue habiendo, por lo tanto, mucha tela que cortar y muchas dificultades y resistencias que vencer para que la UE esté a altura de sus propias ambiciones ante la globalización, ejerciendo su tarea entre los actores globalmente relevantes: "*A player; not only a payer*", solía decir al respecto la antigua *High Rep* Federica Mogherini. Y hacerlo además con la urgencia con que los EEUU, China (con Xi Jingping perpetuado como acreedor financiero de las potencias globales, al frente de un régimen político de partido único, el PCRPCh), Rusia (con el endurecimiento y agresividad de Putin como factor desestabilizador de las democracias occidentales, recurriendo a la desinformación, *fake news* y a las *guerras híbridas*, culminadas con su criminal guerra de agresión contra Ucrania desde febrero de 2022), junto a otras potencias emergidas (Brasil, India… entre otras), reclaman que la UE abandone lo que se ha denominado "edad de la inocencia" y madure aceleradamente hasta ejercer *hard power* en pos de su *autonomía estratégica*.

5.- La relevancia del "Case Law": la jurisprudencia del TJUE

Dicho lo cual, un examen del estado de la cuestión relativa a la apertura (*openness*), transparencia y acceso a los documentos y a la información en la UE requiere tener en cuenta la aplicación efectiva del principio establecido en el TL sobre el conjunto de los ámbitos materiales sobre los que se ciernen sus mandatos vinculantes desde el Derecho europeo. A saber: a) El *Case Law* o la jurisprudencia seleccionada del TJUE. Y ello exige repasar el impacto de la transparencia sobre el procedimiento

[29] Cfr. MARTÍN MARTÍNEZ, M.M. (2014: 767-804) y GARCÍA MAHAMUT, R. (2016: 211-218).

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

legislativo; y su impacto sobre los procedimientos jurisdiccionales ante el propio TJUE; b) Los procedimientos de infracción (*infringement procedures*) incoados por la Comisión (singularmente en el caso de los *EU Pilot Cases*); y c) La obligada protección de la privacidad y la confidencialidad de los datos personales en el ámbito de las relaciones internacionales de la UE[30].

Y de ese examen se desprenden algunas enseñanzas útiles para el fortalecimiento del carácter vinculante del TL y la CDFUE, especialmente en lo que concierne a sus disposiciones orientadas a reforzar la participación ciudadana y la dación de cuenta (*accountability*) en las instituciones de la UE.

En el marco del acceso a documentos en el curso de los procedimientos administrativos de las Instituciones europeas, la jurisprudencia relevante del TJUE (v. *Case Sweden vs Commision*, C-506/08) perfila el denominado "*Public Interest Test*" (interés público en la apertura y el acceso, directamente incidente en la "legitimación democrática" de la UE por vía de la *accountability*). No obstante, en la práctica se establecen excepciones sobre la presunción de que la revelación o acceso con publicidad de algunas determinadas piezas documentales pudieran perjudicar algún interés legítimo igualmente protegido por el Reglamento 1049/2001 (*Case Commission vs Editions Odile Jacob*, C-104/2010, entre otros). La presunción de este carácter ha venido reconociéndose de manera paulatina en materias tan variadas (pero sensibles para la esfera de toma de decisión que corresponde a la Comisión) como las relativas a las ayudas de Estado, procedimientos de infracción y reglas de competencia. Más recientemente, el TJUE ha ampliado el círculo de la reserva frente al principio general de acceso a los documentos para extenderlo a aquéllos que integran el preceptivo expediente de "*Impact Assesment*" ("Evaluación de Impacto") previo a la iniciativa legislativa que corresponde a la Comisión (*ClientEarth vs. Commission*, T-424/14; *Philip Morris vs. Commission*, T-18/15, entre otros).

En cuanto al acceso a los documentos obrantes en poder del propio TJUE en el curso de sus procedimientos jurisdiccionales, el art. 15 TFUE establece la regla general de que el principio de acceso sólo resulta aplicable a los documentos de carácter administrativo, no a las deliberaciones decisivas sobre la resolución del caso y determinantes del fallo. (T-188/12, *Breyer vs Commission*).

Los procedimientos de infracción incoados por la Comisión han sido singularmente excepcionados de la regla de acceso a los documentos en el *Case Law* del TJUE (C-504/11 y C-605/11 *LPN and Finland vs Commission*), línea jurisprudencial que se ha extendido a los elementos relevantes de la adjudicación de los *EU-Pilot Projects* (Proyectos Piloto europeos, financiados por la Comisión).

[30] Seguimos, en este punto, a CURTIN, D., LEINO-SANDBERG (2017).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

Pero, seguramente, donde mayor incidencia reviste la jurisprudencial del TJUE a la hora de excepcionar la regla general de transparencia y acceso a los documentos, es en la protección de la privacidad (derecho fundamental a la "vida privada" y a la confidencialidad de los datos relativos a la personalidad (art. 16 TFUE y arts. 7 y 8 CDFUE), vista la transcendencia de su consagración como "derechos fundamentales" de cualesquiera personas sobre las que las instituciones de la UE puedan ejercer sus atribuciones). Se trata aquí del equilibrio (ponderación de bienes) que en todo ordenamiento regido por principios constitucionales requiere la convivencia entre los derechos a la libertad y a la seguridad (art. 6 CDFUE, como es el caso también de la Constitución española de 1978, Preámbulo y art. 17 CE) en su acepción específica de impacto sobre el derecho de acceso a la información pública (art. 42 CDFUE, arts. 20 y 105 CE) y garantía del derecho a la privacidad (arts. 7 y 8 TFUE, art. 18 CE).

El art. 4.1.b) del Reglamento 1049/2001 exceptúa expresamente del acceso a los documentos a aquéllos que puedan lesionar el derecho a la vida privada y a la integridad personal conforme al Derecho europeo de protección de datos (antigua Directiva 46/95, de Protección de Datos; Reglamento 45/2001 de Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales por las Instituciones y Organismos Comunitarios; y, sobre todo, el *Data Protection Package*, compuesto por el Reglamento 679/2016 y la Directiva 680/2016, plenamente en vigor desde el 18 de mayo de 2018).

Como es conocido, el *Paquete de Protección de Datos* (cuya pieza principal es el llamado *GDPR* en la jerga europea, definitivamente adoptado por el PE en 2016 y cuya entrada en vigor se completa en 2018) incorpora un formidable avance en el nivel de protección de la privacidad en la UE y en sus EEMM. No en vano, no se pierda de vista, se deroga una Directiva en favor de un Reglamento, norma directamente aplicable sin necesidad de transposición por la legislación nacional, plenamente vinculante para los EEMM (y para sus entidades y empresas) e invocable por los ciudadanos ante los Tribunales y Juzgados de sus Poderes Judiciales.

Además de actualizar el Derecho ante la vertiginosa revolución tecnológica y digital que ha tenido lugar en los últimos 25 años (los que median entre la Directiva del 95 y el Paquete de 2018), el *Data Protection Package* refuerza potentemente el principio de consentimiento y los derechos de acceso, rectificación y cancelación (con la introducción incluso del novedoso "derecho al olvido"; "*right to be forgotten* "), al mismo tiempo de incrementar las sanciones a las entidades y empresas incumplidoras y las obligaciones de atenimiento a las reglas y procedimientos de garantía y supervisión en cuanto a protección de datos conforme a la nueva normativa. Se entiende, pues, fácilmente, que el nuevo régimen jurídico eleva considerablemente los estándares de reconocimiento del principio de consentimiento que había fijado años antes el Reglamento 1049/2001.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

El *Case Law* del TJUE a este respecto puede sintetizarse en la doctrina que discurre entre el T-309/97, *Bavarian Lager vs. Commission,* al T-115/13 *Dennekamp vs European Parliament* y C-665/13 *CientEarth and PAN Europe vs EFSA*.

Merece singular atención la jurisprudencia del TJUE que perfila la excepción de la regla general de acceso a los documentos que afecta a las negociaciones de acuerdos internacionales conforme a las atribuciones internacionales de la UE, especialmente a la luz de la nueva concepción que el TL ha imprimido a la diplomacia europea, al *Servicio Europeo de Acción Exterior* y a la *Política Exterior, de Seguridad y Defensa*[31].

El primer caso relevante resuelve la demanda interpuesta en su día por Sophie In't Veld, eurodiputada neerlandesa en la Comisión LIBE (del Grupo ALDE, liberal), contra el Consejo, requiriendo pleno acceso a los informes del Servicio Jurídico del Consejo sobre las negociaciones en curso para la conclusión del llamado "*acuerdo SWIFT*" entre la UE y los EEUU (en rigor, TFTP: *Tracking of financiation of Terrorism Program*), T-529/09 *Sophie In't Veld vs. the Council supported by the Commission*, asunto en el TG desautoriza al Consejo, y C-350/12 *Council vs. Sophie In´t Veld*, en que el Consejo vuelve a perder el caso contra la eurodiputada). La jurisprudencia asentada en este asunto se resume en el principio de que la regla de la transparencia no puede ser excluida en los asuntos internacionales en la medida en que una decisión de apertura de negociaciones pueda conducir a un acuerdo que tenga impacto en la actividad legislativa de la UE. El Consejo, como el resto de las instituciones, al adoptar la decisión de mandatar a la Comisión la negociación de un acuerdo, debe ponderar este impacto a la hora de determinar cuáles de los documentos deben ser preservados del conocimiento público –especialmente cuando afecten a la privacidad y a los datos personales, derecho fundamental protegido por al CDFUE– y cuáles pueden desvelarse.

La misma eurodiputada, miembro de la Comisión LIBE, Sophie In't Veld, planteó otro caso ante el TJUE con ocasión de la negativa por parte de la Comisión a su requerimiento de acceso a la documentación de los borradores del Acuerdo Internacional contra las Falsificaciones comerciales (*Anti-Couterfeiting Trade Agreement*). El TG delimita su doctrina, concediendo la excepción relativa a aquellos documentos que en una negociación en curso requieran razonablemente especial celo y discreción ("*particular care and discretion*"). T-301/10, *Sophie In't Veld vs Commission.* Se inscribe esta matización de su doctrina jurisprudencial en la confidencialidad y la confianza mutua que resultan requeribles en las negociaciones entre varios actores internacionales, cuyo quebrantamiento por excesiva exposición (*disclosure*) de las ofertas negociadoras y posiciones en curso pudiera perjudicar los intereses públicos en las relaciones internacionales.

[31] Cfr. GOSALBO BONO (2015: 231-320).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

Un tercer asunto digno de mención es el que fue planteado por el profesor Leonard Besselink, quien, en el curso de una investigación académica, requirió al Consejo el mandato de negociación por el que se autoriza a la Comisión a negociar el Acuerdo de Adhesión de la UE al CEDH (conforme a lo establecido en el art. 6.2 TUE, negociación sobre la que el PE se pronunció favorablemente en su Resolución de 2013, aunque finalmente encalló ante la sentencia en contrario del TJ, Dictamen 2/2013)[32]. Aunque el TJ declaró que, aunque en este caso concreto, el Consejo había asumido una interpretación excesivamente amplia de las excepciones disponibles, las partes negociadoras (la UE, de un lado, y el Consejo de Europa, de otro) pueden preservar de la publicidad (en la web) las posiciones negociadoras que puedan perjudicar el intercambio y la aproximación de opciones y contraopciones en la interlocución directa. En conclusión, aunque el TJUE muestra sensibilidad respecto a los requerimientos de la discreción y confianza que deben regir las mesas de una negociación, el equilibrio entre el interés público en las relaciones internacionales y la regla de transparencia deben contenerse dentro de los límites tan estrechos como resulte razonablemente posible.

Por último, visto todo lo anterior, en este marco de *Case Study* sobresale también, por su interés, una sentencia del TJUE (Tribunal General) de 22 de marzo de 2018: el *Caso De Capitani vs. Parlamento Europeo*. Emilio de Capitani fue el funcionario del PE que, durante mi primer mandato como Presidente de LIBE, ejerció la jefatura del Secretariado de esta Comisión Parlamentaria (Letrado mayor, diríamos en Derecho parlamentario español). Tras su jubilación, decide investigar académicamente los procedimientos legislativos en curso en la Comisión LIBE, y solicita (y se le deniegan) documentos relevantes para la realización de esos estudios[33].

En el asunto en especie, el TG afronta el examen del alcance jurídico de la regla de transparencia y del derecho de acceso a documentos de la UE. Enjuicia desde el parámetro de los derechos de la CDFUE –y no lo hace por primera vez– los mandatos del Reglamento 1049/2001. Analiza desde esos parámetros de validez los artículos del TFUE y del reglamento interno del Parlamento Europeo (*Rules of Procedure*) los preceptos relativos a la accesibilidad de los documentos obrantes en un determinado procedimiento legislativo en curso; particularmente, se centra su pronunciamiento sobre la documentación relevante en la denominada "*fase de trílogo" ("diálogos tripartitos* ") y, aún más concretamente, a los "cuadros de cuatro columnas" en que se contrastan las ofertas negociadoras de cada institución en la fase más avanzada (y tendencialmente final) del *iter legislativo*, en que PE y Consejo

[32] Cfr. MARTÍN Y PÉREZ NANCLARES, J. (2013: 826-869) y MARÍN ASÍS, J.R. (2013).

[33] Sentencia del TJUE, de 22 de marzo de 2018, en el Asunto T-540/15, De Capitani contra el Parlamento Europeo. Esta jurisprudencia ha tenido continuidad en el *Asunto De Capitani II* (TG, 25 d enero de 2023).

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

deben encontrar "compromisos" que permitan la aprobación final (segunda lectura en el PE, previo acuerdo del Consejo) y entrada en vigor de la norma.

En este pronunciamiento, el TJUE (TG) arranca de la premisa de que el denominado *trílogo* es, en efecto, una fase decisiva de la legislación europea. La denegación de acceso a su documentación debe ser proporcionada y motivada sobre bases racionales y objetivas, no excesiva ni injustificada si no queda acreditada la preservación de un bien jurídico (confidencialidad de datos personales, consideraciones de seguridad), puesto que, de otro modo incurrirá en contravención de los mandatos generales y específicos de "facilitar el acceso" "velando por el mayor grado de transparencia posible". En consecuencia, en el fallo, el TG anula la Decisión del PE por la que se deniega a Emilio de Capitani el "acceso íntegro" a los documentos LIBE.

6.- Particular referencia a los derechos a la transparencia y acceso a la información en el marco de la lucha contra la corrupción y el blanqueo

En el debate alrededor del *Decision Making y Law Making* de la UE, los avances de la transparencia suelen presentarse aparejados a la lucha contra la corrupción y el blanqueo de dinero procedente de negocios ilícitos. En la Legislatura 2019/2924 del PE y de la Comisión Europea (Comisión VDL) ha tenido lugar el procedimiento legislativo de actualización del Derecho contra el blanqueo de capitales y la financiación del terrorismo. Este Paquete legislativo, conocido en la jerga como "AML VI", fue iniciado por la Comisión VDL en julio de 2021, y su tramitación ha involucrado a varias Comisiones legislativas del PE: concretamente, LIBE y ECON. El objetivo proclamado: incrementar la eficiencia de la respuesta preventiva y represiva de la UE, corrigiendo al mismo tiempo las heterogéneas prácticas aplicativas detectadas en los EEMM (dando lugar a la patología del "*forum shopping*" a la búsqueda de las jurisdicciones más lenitivas y convenientes para los intereses de las tramas corruptas, aspirando como es obvio a su propia impunidad) y reforzando y mejorando la localización e identificación de transacciones sospechosas.

Los trabajos legislativos del PE fijaron, en su momento, como marco temporal para su completamiento la primera mitad de 2023 (Presidencia sueca del Consejo de la UE), aunque, como era previsible, alcanzaran finalmente a la Presidencia española (segunda mitad de 2023).

El Paquete AMLVI comprende, en primer lugar, un nuevo Reglamento AML, instrumento normativo con normas directamente aplicables y vinculantes por ende para los EEMM al fin de asegurar una mayor convergencia y armonización de las normas AML/CTF en toda la UE. Sigue, en segundo lugar, una nueva Directiva AML orientada a mejorar la convergencia de las prácticas de los supervisores nacionales y de las respectivas *Unidades de Inteligencia Financiera* (UFI) para lo que se requiere una mayor cooperación entre Autoridades nacionales competentes en la lucha contra el blanqueo. Uno y otros actos normativos plantean cuestiones pendientes,

CC BY SA

DOI: https://doi.org/10.51915/ret.305

como la cobertura de altos patrimonios expuestos a "factores de alto riesgo" y "bienes de alto valor", conexo al acceso legítimo al registro de beneficiarios efectivos. Figura, en tercer lugar, un Reglamento que establece una nueva Agencia de la UE, la *Autoridad Europea de Lucha contra el Blanqueo de Capitales*, elemento capital del sistema integrado de supervisión de entidades obligadas, con normas armonizadoras y de cooperación con las UFI nacionales de los EEMM. Cumple anotar aquí que una relevante sentencia del TJUE (14 julio 2022) sitúa en pie de igualdad a los dos colegisladores (PE y Consejo) a la hora de fijar la sede de cualquier nueva Agencia o Autoridad europea, a la que subsigue el régimen de su cooperación con Europol. Pero hay todavía dos Reglamentos más en este complejo Paquete normativos: de un lado, el Reglamento sobre Transferencia de Fondos, con reglas de armonización de la información que la acompaña en pos de su trazabilidad, incluyendo los llamados *criptoactivos*; de otro, la nueva Directiva de Acceso a los Registros Centralizados de Cuentas Bancarias mediante el denominado "*Punto de Acceso Único*" (SAP).

Seguramente reside en el régimen jurídico de la fijación de la sede de la nueva *Autoridad Europea contra el Blanqueo de Capitales* el punto de mayor interés en cuanto novedoso. Por primera vez una sentencia del TJUE (14 julio 2022, en los asuntos acumulados sobre la ubicación de la Agencia Europea del Medicamento y de la Autoridad Laboral Europea) dictamina con claridad que no corresponde en exclusiva a los EEMM (por medio de "común acuerdo" alcanzado en el Consejo, art.341 TFUE) la fijación de las sedes de los Entes y Organismos creados por Derecho de la UE, sino al "legislador," en un concepto que incluye inequívocamente al PE. El Consejo asume el impacto de la sentencia, adoptando una nueva metodología para la valoración de las candidaturas presentadas, subseguida, por su parte, por la conformación de un equipo negociador para la elaboración de su propio método de aproximación a "criterios objetivos de selección" y "lista corta" de candidaturas para acometer posteriormente la fase definitiva en las correspondientes negociaciones interinstitucionales con el Consejo.

7.- Consideraciones conclusivas

La conclusión es meridiana. Importa tener en cuenta los principios configuradores del objeto que nos ha ocupado a lo largo de estas páginas. Las reglas del Derecho europeo concernientes a la transparencia y al acceso a los documentos han de ser conjugadas con las de los derechos y libertades protegidos por la CDFUE (acceso libre a la información, vida privada, confidencialidad, derecho a la buena administración y al buen gobierno), pero también con las normas que fijan los procedimientos internos de toma de decisiones en las instituciones europeas.

Desde los primeros trazos del proyecto en que la UE adquiere dimensión política y rasgos constitucionales (esto es, desde el *TUE de Maastricht* de 1992 hasta el TL en 2009, pasando por el *Tratado de Ámsterdam* de 1997 y el *Tratado de Niza* de 2000),

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

las tres instituciones basales de la arquitectura política (Consejo, Comisión y Parlamento Europeo) han venido vinculándose al conjunto de reglas y principios que en el transcurso de los años han adquirido su perfil más actual y exigente (Directiva 45/96, de Protección de Datos, Reglamento 1049/2001, de Transparencia y Acceso a los Documentos, Reglamento 45/2001, de Protección de personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, y Reglamento 679/16 de Protección de Datos, junto con la Directiva 680/16, de Protección de Datos en la Investigación de los Delitos y en la persecución del Crimen).

De modo que, de consuno, su primer efecto normativo apunta a una potente expansión del principio de acceso a los documentos tanto en los procedimientos administrativos como en los legislativos, así como en las negociaciones que la Comisión conduzca por mandato del Consejo. Si bien en los primeros tiempos de la construcción europea tales procedimientos adquirieron una reputación negativa por su alegado "oscurantismo" ("*behind doors, behind the scenes"*) y su carácter tecnocrático –así por lo menos resulta en la narrativa común de lo que denominamos "*conventional wisdom* ", generalmente asumidas aun cuando careciendo de contraste empírico o de base racional–, tanto el énfasis puesto en la acepción "deliberativa" y "participativa" de la democracia representativa, como la elaboración por el TJUE –*pretoriana*, se la llama– de un cuerpo de derechos y libertades vinculantes para las instituciones, organismos y agencias de la UE, han acabado abriendo paso a una jurisprudencia y doctrina vinculantes respecto de los principios de transparencia y acceso.

Es cierto, sin embargo, que tras la entrada en vigor del TL se produjo una expectativa de actualización y refuerzo del ya vigente Reglamento 1049/2001. Los trabajos y debates que tuvieron lugar durante la Legislatura 2009-2014, en la que fui Presidente de la Comisión LIBE, no consiguieron culminar con su revisión ni tampoco modificar aquellos aspectos más insatisfactorios o expuestos a contornos deletéreos. Algunos casos judiciales (*Case Law*) planteados ante el TJUE por miembros de la propia Eurocámara (la secuencia de los casos Int'Veld) ilustran las dificultades de la aplicación a este ámbito del principio de la "leal cooperación" entre las instituciones (art. 13 TUE) cuando se trata de aplicarlo a la transmisión y/o acceso documental, así como al perfilamiento de las situaciones y supuestos en que su rigurosa observancia resulte necesaria para el correcto desempeño de las funciones de control y de legislación que corresponden al PE.

Tampoco quiere ello decir que el derecho de acceso resulte garantizado con carácter general a toda la ciudadanía (de forma indeterminada o indiscriminada). Ni siquiera cuando se trata de documentos obrantes en los procedimientos parlamentarios internos (reglados en las *Rules of Procedure*, el equivalente al Reglamento parlamentario en España, art. 72 CE), en la medida en que algunos afecten a los mecanismos de negociación interna, composición de intereses o

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

confidencialidad de las comunicaciones personales (de los eurodiputados/as y de los *Grupos Políticos*).

Es claro, visto lo anterior, que la actual redacción del vigente Reglamento 1049/2001 debería ser revisada para actualizar sus preceptos, en todo, al TL y CDFUE, cuyo alcance normativo se extiende sólo con matices a las demás instituciones (incluyendo al BCE y al BEI) y agencias (en lo que sea de aplicación, también a Eurojust y Europol, conforme a sus propios Reglamentos *lisbonizados*, así como a la ya aprobada Fiscalía Europea, *ex* art. 86 TFUE)[34].

Tampoco resulta, por su parte, del todo satisfactoria la situación concerniente al acceso a documentos por parte del propio TJUE y las actuales excepciones de las que se benefician el BCE, el BEI y las agencias especializadas (cooperación judicial y cooperación policial, junto a la Fiscalía Europea). El derecho a un "juicio público" con todas las garantías (art. 47 CDFUE) es inequívocamente un derecho fundamental de primerísimo rango. Con todas las consecuencias que resulten razonables en su ponderación con los demás derechos (especialmente en lo que atiene a los de la privacidad, arts. 7 y 8 CDFUE).

Ha de recordarse, al respecto, que tanto las relaciones internacionales como la protección de la privacidad y la confidencialidad de los datos personales son excepciones contempladas en la actual redacción del vigente Reglamento 1049/2001. Pero también que tanto la jurisprudencia del TJUE como la propia CEDH (y jurisprudencia del TEDH) restringen progresivamente el margen de restricción del acceso y la transparencia. Asimismo, el propio Ombudsman europeo (la *Ombudsperson* Mary O'Reilly) ha abogado por la extensión y garantía de estas reglas en contextos delicados como indudablemente son los que afectan a las relaciones internacionales, máxime cuando afecten a negociaciones en curso, incluso (como ha sido el caso en más de una ocasión en estos últimos años) cuando ello impacte en asociaciones estratégicas con otros actores globales como es el caso del llamado "diálogo transatlántico entre la UE y EE.UU" *(casos Swift, Umbrella Agreement, Privacy Shield, US-EU PNR*, entre otros…)[35].

En suma, nadie debe ignorar que el equilibrio a asegurar entre transparencia, acceso y derechos fundamentales no debe perder de vista el carácter constitucional e indisponible de éstos de acuerdo con la CDFUE y con la jurisprudencia del TJUE que los eleva a parámetro de validez en el enjuiciamiento de todo el Derecho europeo. Allí donde el desvelamiento de lo que tradicionalmente había sido considerado como "secreto" o "reservado" no afecte a la privacidad ni al interés preponderante

[34] Cfr. ESCALADA LÓPEZ, M. (2014: 89-127).

[35] Véase LÓPEZ AGUILAR (2017 b).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia, un derecho europeo…
por Juan Fernando López Aguilar
Págs. 23-49
DOI: https://doi.org/10.51915/ret.305

de la seguridad y la lucha contra el crimen, el principio de transparencia debe obrar su trabajo.

Si a esta síntesis sumamos el contundente impacto de la entrada en vigor del *Data Protection Package* (Reglamento 679/16 y Directiva 680/16), y el seguimiento de su incorporación por los EE.MM de los que debe entender el *European Data Protection Supervisor* y el *European Board of Data Protection Authorities* (antiguo Art. 29 *Working Party* de la anterior Directiva 46/95), cabe albergar expectativas todavía positivas de que el bloqueo (y frustración) de los debates transcurridos en la pasada Legislatura del PE 2009-2014 (que fue además la inaugural del TL, que entró en vigor en 2009) puedan abrirle paso a una actualización que sigue siendo requerida y, por tanto, aconsejable.

El escenario deseable para un futuro mediato debe apuntar al diseño y configuración normativa de un conjunto homogéneo de *reglas de clasificación de documentos europeos* ("secretos" o "reservados") para todas las instituciones, organismos y agencias de la UE, en una legislación en la que el PE actuara como legislador europeo en un ámbito tan sensible como es el que concierne al desarrollo de los derechos fundamentales de la ciudadanía contenidos en la CDFUE. Subyace a este reto, cómo no, la dificultad impuesta por la heterogeneidad de las leyes nacionales sobre *secretos oficiales* de los EE.MM. (junto a las considerables diferencias históricas en cuanto a las condiciones de su régimen jurídico en cada situación nacional en el conjunto de la UE).

En cuanto a las reflexiones y propuestas prospectivas que pueden surgir del análisis que hemos seguido hasta ahora, cabe, en lo que nos importa, concluir al menos lo siguiente: La Legislación europea sobre transparencia y acceso a los documentos actualmente vigente se encuentra desfasada, en claro defecto de acompasamiento con el desarrollo de los objetivos planteados por el TL y con los avances tecnológicamente. Desde el punto de vista normativo, el actual *status quo* resulta insatisfactorio en la medida, manifiesta, en que se acentúa la distancia entre los objetivos enfáticamente asumidos en el TL y en la CDFUE y las realizaciones políticas y normativas completadas hasta hoy. Debería aun reducirse, significativamente, el margen de maniobra para las restricciones de los derechos de acceso a documentos de la UE que resultan arbitrarias, carentes de fundamento legítimo y objetivable o no suficientemente justificadas.

El Reglamento 1049/2001, de *Transparencia y Acceso a los documentos de la UE*, debe, por consiguiente, asegurar su adecuación –a la espera de la próxima modificación legislativa, y ojalá que cuanto antes– a los mandatos del TL y la CDFUE. La regla de la transparencia debe impactar también sobre los procedimientos administrativos de todos y cada uno de los cauces jurisdiccionales seguidos ante el TJUE (TFP de la UE, TG y TJ). La jurisprudencia del TJUE, singularmente en la sentencia *Capitani vs. PE*, vincula inequívocamente el procedimiento legislativo a las

CC BY SA

DOI: https://doi.org/10.51915/ret.305

reglas de la transparencia incluso en la fase de *trílogos* ("negociaciones tripartitas"). Y cobran aquí nueva fuerza, con argumentos convincentes, las posiciones que abogan por la actualización y adecuación del Reglamento 1049/2001 respecto de los mandatos del TL y CDFUE. Las herramientas tecnológicas (*websites*) promueven y facilitan nuevos espacios de apertura a la regla de transparencia. Los documentos administrativos relativos a los procedimientos de negociación política de Tratados –y, consiguientemente, a tan sensible aspecto de las relaciones internacionales– deben sujetarse también a la regla de transparencia, restringiendo en lo posible las consideraciones que tengan un carácter de excepción.

A modo de conclusión, el equilibrio entre transparencia y protección de datos debe ser preservado en cualesquiera circunstancias, pese a las dificultades y conforme a las exigencias planteadas por la entrada en vigor del TL y CDFUE. Lo que se traduce, en la práctica, la superación de la antigua normativa en la materia, previa al TL de 2009 (Directiva 95/46, de *Protección de Datos*, Reglamento 45/2001, de *Protección de las Personas Físicas ante el Tratamiento de Datos Personales por las Instituciones y Organismos europeos*; Directiva 24/2006 de *Conservación de Datos/ Data Retention*, entre otros elementos…) y su derogación o desplazamiento por un *Paquete* normativo consistente y adaptado a la consagración de la CDFUE como parámetro de validez de todo el Derecho Europeo. El *Data Protection Package* (GDPR, en jerga comunitaria), compuesto por el Reglamento 679/2016, de *Protección de Datos*, y la Directiva 680/2016, de *Tratamiento de Datos en la Prevención y persecución del crimen y de Protección de Datos en la Investigación de los Delitos* (dirigida a las *Law Enforcement Agencies:* Cuerpos de Policía, Judicatura, Fiscalía).

Sistémicamente, en su conjunto, la nueva legislación europea que deba ser adoptada en un futuro mediato debería asegurar, con mayor fuerza que nunca antes, una ponderación proporcionada y adecuada de la confidencialidad, el secreto y la clasificación de documentos en su conjugación con las reglas de apertura, transparencia y acceso a los documentos.

Bibliografía

ABRISKETA URIARTE, J. 2017. "La dimensión externa del derecho de la UE en materia de refugio y asilo: un examen desde la perspectiva del non-refoulement". *Revista de Derecho Comunitario Europeo,* núm. 56: 119-158.

ANTONINO DE LA CÁMARA, M. 2017. "Transparencia y derecho de acceso a la información versus protección de datos". *Revista Internacional de Transparencia e Integridad*, núm.4, mayo-agosto 2017: 1-20.

BARON CRESPO, E. 2006. *Constitucionalización del poder legislativo de la UE*. Madrid: Civitas.

CC BY SA

DOI: https://doi.org/10.51915/ret.305

CERRILLO I MARTÍNEZ, A. 2017. "El difícil equilibrio entre transparencia pública y protección de datos personales". *Cuadernos de Derecho Local*, núm.45, octubre: 127-156.

CURTIN, D., LEINO-SANDBERG, P. 2017. *Openness, Transparency and the Right of Access to Documents in the EU*. In-depth analysis. Bruselas: Petitions Committee, European Parliament.

DI FEDERICO, G. (Ed.) 2011. *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*. Londres: Springer.

ESCALADA LÓPEZ, M.L. 2014. "Los instrumentos de cooperación judicial europea. Hacia una nueva Fiscalía Europea". *Revista de Derecho Comunitario Europeo*, núm. 47: 89-127.

GARCÍA MAHAMUT, R.:

-2016. "La ductilidad del derecho a la protección internacional (refugio y protección subsidiaria) ante las crisis humanitarias: un desafío para Europa y para el Sistema Europeo Común de Asilo". *Teoría y Realidad Constitucional*, núm. 38: 211-238.

-2019. "Del Reglamento General de Protección de Datos a la LO 3/2018 de Protección de Datos y Garantía de los Derechos Digitales" en *El Reglamento General de Protección de Datos: un enfoque nacional y comparado* (eds. R. García Mahamut y B. Tomás Mallén), Tirant lo Blanch, Valencia: 95-131.

GARCÍA MAHAMUT, R. y VIGURI CORDERO, J. 2019. "La protección de los datos personales de los solicitantes de protección internacional en el (Nuevo) Sistema Europeo Común de Asilo: Grandes desafíos y graves deficiencias". *Teoría y Realidad Constitucional*, núm. 44: 237-270.

GARZÓN GLARIANA, G. 2015. "El Parlamento Europeo y la evolución del poder legislativo y del sistema normativo de la UE". *Revista de Derecho Comunitario Europeo,* núm. 50: 43-83.

GOSALBO BONO, R. 2015. "Insuficiencias jurídicas e institucionales de la acción exterior de la UE". *Revista de Derecho Comunitario Europeo*, núm. 50: 231-320.

GUICHOT, E. 2023, *El acceso a la información pública en el Derecho europeo*. Valencia: Tirant lo Blanch.

LÓPEZ AGUILAR, J.F.:

- 2013. *La UE: suicidio o rescate: del mito del rapto a Europa a la tentación de la autodestrucción*, Madrid: Tirant lo Blanch.

- 2017 a). *Europa: Parlamento y Derechos: Paisaje Tras la Gran Recesión*. Madrid: Tirant lo Blanch.

CC BY SA

DOI: https://doi.org/10.51915/ret.305

- 2017 b). "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU". *Teoría y Realidad Constitucional*, núm. 39: 557-581.

-2020. *El Parlamento Europeo. Una experiencia única*. Las Rozas: Wolters Kluwers.

MARÍN ASÍS, J. R. 2013. *La participación de la UE en Tratados Internacionales para la Protección de los Derechos Humanos*. Madrid: Tecnos.

MARTÍN MARTÍNEZ, M.M. 2014. "Límites a la libre circulación de personas en la UE por razones de orden público, seguridad o salud pública en tiempos de crisis: una revaluación a la luz de la jurisprudencia del TJUE". *Revista de Derecho Comunitario Europeo*, núm. 49: 767-804.

MARTÍN Y PÉREZ NANCLARES, J. 2014. "El TJUE pierde el rumbo en el dictamen 2/13: ¿merece todavía la pena la adhesión de la UE al CEDH?". *Revista de Derecho Comunitario Europeo*, núm. 52: 826-869

MUÑOZ MACHADO, S. 2015: "Los tres niveles de garantías de los Derechos Fundamentales en la UE: problemas de articulación". *Revista de Derecho Comunitario Europeo,* núm. 50: 195-230.

VIGURI CORDERO, J. 2020. "La Seguridad Nacional y la excepción en el Sistema Europeo Común de Asilo (SECA)". *Revista de Derecho Político*, núm. 107: 303-335.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

El conflicto entre la transparencia y la protección de datos tras la entrada en vigor del Reglamento General de Protección de Datos

Manuel Medina Guerrero[1]
Catedrático de Derecho Constitucional
Universidad de Sevilla
España

ORCID: 0000-0002-2227-813X

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

El presente artículo se ha realizado en el marco del proyecto de investigación del Ministerio de Ciencia e Innovación DATATRANSCO con referencia n.º PID2021-128309NB-I00.

RESUMEN: La entrada en vigor del Reglamento General de Protección de Datos ha supuesto un cambio notable en el marco normativo europeo regulador del derecho fundamental a la protección de datos. En particular, ha conllevado un cierto avance en la regulación del conflicto entre este derecho fundamental y el derecho de acceso a los documentos públicos. El principal objetivo de este trabajo es examinar si es recomendable o incluso exigible que se modifique la Ley de transparencia, acceso a la información pública y buen gobierno, a fin de acomodarla a este renovado marco normativo europeo. A este respecto, el trabajo aporta algunas sugerencias de reforma de la citada Ley que garantizarían su más adecuado encaje con el Reglamento General de Protección de Datos.

PALABRAS CLAVE: Derecho de acceso a la información pública, derecho a la protección de datos personales, transparencia, derecho fundamental, Reglamento General de Protección de Datos.

[1] Catedrático de Derecho Constitucional de la Universidad de Sevilla (desde 2006). Letrado del Tribunal Constitucional (1994-1998). Director de la Fundación Democracia y Gobierno Local (mayo 2004-septiembre 2010). Miembro de la Comisión que elaboró el "Libro Blanco para la reforma del gobierno local" (Ministerio de Administraciones Públicas, 2004-2005). Miembro de la Comisión de Expertos Independientes del Pacto Antitransfuguismo (2010-2014). Vocal de la Junta Electoral de Andalucía (diciembre 2003-julio 2014). Ha sido Director del Consejo de Transparencia y Protección de Datos de Andalucía.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

CONTENIDOS: 1.-Introducción. 2.-La función de armonizar el acceso a la información pública y la tutela de datos personales en el Reglamento General de Protección de Datos. 3.-La cláusula de apertura del artículo 85 RGPD. El derecho a acceder a la información pública por parte de los periodistas. 4.-El artículo 15 LTAIBG en el contexto del RGPD. *4.1.-Los criterios de ponderación del apartado tercero del artículo 15 LTAIBG. 4.2.-El acceso a la información relativa a infracciones administrativas.* 5.-La LTAIBG como ley parcialmente orgánica.- Bibliografía.

The conflict between transparency and data protection after the entry into force of the general data protection regulation

ABSTRACT: The entry into force of the General Data Protection Regulation has brought about a significant change in the European regulatory framework governing the fundamental right to data protection. In particular, it has led to some progress in regulating the conflict between this fundamental right and the right of access to official documents. The main objective of this paper is to examine whether it is advisable or even required to amend the Law on Transparency, Access to Public Information and Good Governance, in order to adapt it to this renewed European regulatory framework. In this regard, the paper provides some suggestions for the reform of Article 15 of the aforementioned Law that would ensure a more appropriate fit with the General Data Protection Regulation.

KEY WORDS: Right of access to public information, right to the protection of personal data, transparency, fundamental right, General Data Protection Regulation.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

1.- Introducción

Entre los diez compromisos asumidos por el Ejecutivo en el *IV Plan de Gobierno Abierto*, el primero de ellos consiste precisamente en modificar el marco regulatorio de la transparencia, que incluye, entre otros aspectos, la reforma de la propia Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno (en adelante, LTAIBG). El objetivo de las siguientes líneas es plantear -como hipótesis de trabajo- si, en el marco de dicha prometida reforma, sería conveniente o necesario efectuar algún retoque en la Ley 19/2013 a fin de acomodarla al Reglamento General de Protección de Datos[2], que comenzó a aplicarse a partir del 25 de mayo de 2018 (artículo 99.2).

Como es sabido, al abordar la regulación de la cuestión capital de establecer el sistema de límites de la transparencia, el legislador optó por dedicar de forma específica un artículo al límite que cabía esperar generase más conflictos en la práctica, a saber, el derecho fundamental a la protección de datos personales. Su artículo 15, en efecto, fija reglas, principios y criterios llamados a orientar al operador jurídico que debe ciertamente dar respuesta a las solicitudes de información, pero que al unísono está también obligado a no soslayar la tutela de los datos de carácter personal. Un entramado de reglas y criterios de ponderación que asimismo resultan de aplicación cuando de obligaciones de publicidad activa se trata (art. 5.3 LTAIBG).

Este sistema de resolución de conflictos entre transparencia y protección de datos, que ha funcionado razonablemente bien durante estos años, se erigía y fundamentaba -como no podía ser de otra manera- sobre la normativa entonces existente reguladora del derecho fundamental a la protección de datos personales: la Directiva 95/46/CE y la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que vino a trasponer dicha Directiva. De hecho, el referido art. 15 LTAIBG, en la medida en que fija y concreta el alcance y determinados límites del derecho fundamental *ex* art. 18.4 CE, y por tanto aborda la regulación de una materia reservada a ley orgánica, debió aprobarse con tal carácter. Por consiguiente, las numerosas decisiones de los órganos independientes de control de la transparencia que han resuelto la miríada de controversias suscitadas al respecto se han fundamentado en una disposición cuya suficiencia de rango normativo puede plantear dudas en algunos de sus aspectos. Pero no podemos ahora detenernos en este punto, al que tendremos que volver siquiera incidentalmente más adelante.

Pues la finalidad central de estas páginas -como decíamos- no es otra que valorar si y en qué medida la entrada en vigor del Reglamento General de Protección de Datos (que, aunque heredero de la Directiva 95/46/CE, aporta notables novedades) perfila

[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.

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

un renovado marco normativo que permite -o aun exige- retocar el sistema de resolución de conflictos contenido en el art. 15 LTAIBG.

2.- La función de armonizar el acceso a la información pública y la tutela de datos personales en el Reglamento General de Protección de Datos

Pues bien, lo primero que debe reclamar nuestra atención es que, a diferencia de la Directiva 96/46/CE, el RGPD sí dedica un específico precepto -el art. 86- de su Capítulo IX ("Disposiciones relativas a situaciones específicas de tratamiento") al "tratamiento y acceso del público a documentos oficiales". Concretamente, este artículo 86 RGPD dice así:

"Los datos personales de documentos oficiales en posesión de alguna autoridad pública o un organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento".

Como es palmario, la tarea de conciliación a la que alude el transcrito precepto es precisamente la que se acometió en la práctica en el art. 15 LTAIBG con base en el anterior marco normativo europeo, la referida Directiva 95/46/CE, la cual, aunque no llevó este asunto a su articulado, sí hizo alguna mención al mismo en su Considerando 72: "la presente Directiva autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva".

Pero volviendo al art. 86 RGPD, parece incuestionable a la vista de su tenor literal que nos hallamos en presencia de una de las numerosas cláusulas de apertura facultativas que jalonan el Reglamento, en cuanto permite a los legisladores nacionales, si así lo estiman oportuno ("podrán"), regular cómo se armoniza el acceso a los documentos públicos con el derecho a la protección de los datos personales. Sencillamente, el legislador europeo optó por no abordar él mismo la regulación de esta cuestión, dejando la misma en manos de los diversos Estados miembros. El precepto, sin embargo, no aclara en modo alguno cuál es el margen de maniobra que se confía sobre el particular a los Estados, e invita sobre todo a cuestionarse si autoriza eventuales "matizaciones", "desviaciones" o, incluso, abiertas divergencias con lo dispuesto en el propio RGPD.

Así, sobre la base de entender que el art. 86 RGPD atribuye a los Estados la competencia para resolver esas colisiones determinado cuál de los dos bienes en conflictos ha de ser prevalente en los diferentes supuestos, se ha sostenido que el propio RGPD exime a los Estados del cumplimiento de sus requisitos y de la obligación de alcanzar el nivel de protección que proporciona con alcance general a los datos personales (Kühling *et al.* 2016: 296).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.306

Otras posiciones, sin duda mayoritarias, se escoran al extremo opuesto, llegando incluso alguna de ellas a poner en cuestión su verdadero valor normativo[3]. Naturalmente, bajo este prisma, se coincide en concluir que el art. 86 RGPD en modo alguno autoriza a los Estados a adoptar reglas que exceptúen o contradigan lo dispuesto en el propio Reglamento. A este resultado llegan fundamentándose en diversas líneas interpretativas.

Por un lado, se recurre al propio tenor literal del precepto para defender la entera sujeción de los Estados a lo establecido en el RGPD, sin posibilidad de introducir ninguna regulación divergente ("en virtud del presente Reglamento", concluye el art. 86 RGPD); y abunda al respecto el Considerando 154: los Estados "pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento"[4].

Por otra parte, a partir de la afirmación del Considerando 154 según la cual "[e]l acceso del público a documentos oficiales puede considerarse de interés público", este grupo de autores sostiene que, en puridad, el art. 86 RGPD no viene sino a reiterar o recordar la base jurídica legitimadora del tratamiento contenida en el art. 6.1.e) RGPD: "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público". Por consiguiente, en la medida en que no atribuye a los Estados ninguna capacidad normativa que no pudieran ya desplegar con base en el art. 6.2 y 3 RGPD[5], el art. 86 RGPD no vendría sino a desempeñar una función puramente declaratoria (Herbst 2018: 1168)[6].

Finalmente, en apoyo de esta posición se invoca asimismo la cláusula de apertura establecida en el precedente art. 85 RGPD, que igualmente aborda la conciliación del derecho a la protección de datos personales con otros bienes jurídicos, concretamente con el derecho a la libertad de expresión y de información. Pero, a diferencia del art. 86 RGPD, este artículo 85 sí contempla expresamente la posibilidad de que los Estados establezcan "exenciones o excepciones" de lo

[3] Y en esta línea, a juicio de Herke Kranenborg, el art. 86 RGPD tiene más bien el carácter de un Considerando (2020: 1217].

[4] Así, Pauly (2021: 1081) e igualmente Specht y Bienemann (2018: 1462-1463). Lo cierto es que la versión española del art. 86 RGPD ("en virtud de…") desdibuja la nota de sujeción al Reglamento que sí se refleja con mayor claridad en el Considerando ("de conformidad con…"). De hecho, la literalidad de nuestro Considerando está más próxima a la de otras versiones, como la alemana, que emplea el mismo término en el artículo 86 y en el Considerando 154 ("gemäß…").

[5] Recuérdese que, en relación con los casos de tratamiento previstos en el apartado 1.e), el art. 6.2 RGPD habilita a los Estados a "mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento…, fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del Capítulo IX".

[6] En esta línea, Louisa Specht y Linda Bienemann sostienen que el art. 86 RGPD no permite a los Estados ninguna dispensa de lo dispuesto en el Reglamento, sino únicamente "concretizar" sus previsiones en el sentido de lo establecido en el art. 6.2 y 3 RGPD (2018: 1457).

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

dispuesto en el RGPD, "si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información". La ausencia de cualquier referencia semejante al respecto en el art. 86 RGPD no viene -según estos autores- sino a corroborar que la cláusula de apertura que nos ocupa no permite a los Estados fijar límites al derecho de protección de datos que no estén basados en otros preceptos del Reglamento[7].

Dicho esto, conviene que nos detengamos en la cláusula de apertura del art. 85 RGPD, ya que, por las razones que veremos a continuación, siquiera de forma mediata o indirecta guarda relación con el derecho de acceso a la información pública configurado en la LTAIBG.

3.- La cláusula de apertura del artículo 85 RGPD. El derecho a acceder a la información pública por parte de los periodistas

La necesidad de hallar un adecuado equilibrio entre el derecho a la protección de datos y la libertad de información no ha dejado de estar presente en la actividad del legislador europeo desde que comenzó a regular directamente esta materia. Ya la Directiva 95/46/CE ponía de manifiesto esta preocupación en su artículo 9, dedicado específicamente al "Tratamiento de datos personales y libertad de expresión":

"En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".

Aunque el precepto, en determinados pasajes, se expresaba en términos imperativos ("los Estados miembros establecerán…"), lo cierto es que el artículo 9 en su conjunto permitía interpretar que los Estados podían decidir si establecían, o no, exenciones o excepciones al valorar libremente si eran necesarias para conciliar ambos derechos. Y así parecía desprenderse del Considerando 37:

> "Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales […]".

Comoquiera que sea, lo cierto es que la inmensa mayor parte de los Estados miembros llevó a su correspondiente normativa de transposición de la Directiva este "privilegio periodístico"-siquiera para reiterar en términos generales lo dispuesto en la misma-, siendo España una de las contadas excepciones al respecto pues la Ley

[7] Así, por ejemplo, Herbst (2018: 1170-1171) y Kranenborg (2020: 1216-1217).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, silenció por completo la cuestión.

Como cabía esperar, una previsión semejante a la contenida en el artículo 9 de la Directiva se incorpora también al RGPD, en el artículo 85, aunque su tratamiento dista de ser idéntico. En el Reglamento se refleja con mucha mayor claridad que esa tarea de conciliación constituye un mandato impositivo de legislación que el legislador europeo dirige a los Estados[8]. Así es, este "mandato general de ponderación"(Buchner y Tinnefeld 2018: 1160) entre el derecho a la protección de datos y la libertad de expresión se hace patente desde el momento en que el citado artículo 85 aísla la prescripción, en su apartado primero, de toda conexión con la idea de que el establecimiento de las exenciones o excepciones depende de la decisión discrecional de considerarlas necesarias para la conciliación; referencia a las posibles exenciones o excepciones que ahora aparece individualizada en un concreto precepto (el segundo apartado del art. 85). Como decía, el tenor literal del apartado primero apunta inequívocamente a que se trata de una obligación:

> "Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria".

Y el Considerando 153 subraya el carácter obligatorio de esta tarea para los Estados: "El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información… con el derecho a la protección de los datos personales con arreglo al presente Reglamento". Se trata, pues, de una cláusula de apertura obligatoria, en cuya virtud los legisladores nacionales pueden y deben establecer en la esfera periodística normas específicas que sustraigan a la misma del régimen general fijado por el RGPD.

Pues bien, la falta de desarrollo normativo interno de esta tarea de conciliación entre protección de datos y libertad de expresión e información, de la que ya adolecíamos bajo la Directiva 95/46/CE, se ha prolongado tras la entrada en vigor del RGPD, pues ninguna referencia se hace al respecto en la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), ni en ninguna otra norma interna -salvo error del que escribe-. Es palmario, pues, en nuestro país el incumplimiento por omisión del inequívoco mandato contenido en el art. 85 RGPD.

Este incumplimiento podría paliarse, siquiera de forma parcial y fragmentaria, si la prevista reforma de la LTAIBG se hace eco del singular papel que tienen los profesionales de los medios en cuanto titulares del derecho al acceso a la información pública. Así es; de conformidad con una línea jurisprudencial que hoy puede catalogarse sin circunloquios como absolutamente consolidada, el Tribunal Europeo de Derechos Humanos afirma que la "libertad de información" a la que alude el artículo 10.1 del Convenio comprende, en determinadas circunstancias, el

[8] Para una posición mucho más matizada acerca del carácter imperativo de la regulación de esta conciliación, véase Fernández Rodríguez (2021: 3307-3309).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

derecho de acceso a la información pública tutelado en las correspondientes leyes nacionales reguladoras de la transparencia.

En efecto, a partir de la Sentencia dictada por la Gran Sala en el caso *Magyar Helsinki Bizottság c. Hungría*, de 8 de noviembre de 2016[9], y sobre la base de que la obtención de la información constituye un paso previo esencial para el ejercicio del periodismo y, por tanto, resulta necesaria en el desempeño de la profesión (Sentencia *Rosiianu c. Rumanía*, de 24 de junio de 2014, §§ 61- 63), el TEDH se ha decantado en términos inequívocos por considerar que en estos casos se incide de plano en el derecho a recibir y comunicar información veraz consagrado en el art. 10 del Convenio. Dejando siempre a salvo que el "derecho de acceso a la información no debería aplicarse exclusivamente a… la prensa" (§168), el TEDH destaca en la Sentencia *Magyar* que tiene una particular importancia la circunstancia de que el solicitante actúe en su condición de periodista para determinar si la denegación del acceso implica la afectación del derecho del art. 10 del Convenio. Pues de lo contrario, de no extenderse la protección del derecho a la fase de obtención de datos, no podría desempeñar correctamente su tarea de informar sobre los asuntos de interés público y, por tanto, cumplir con la función esencial que desempeña la prensa en una sociedad democrática (§§ 164-167). En consecuencia, la negativa a proporcionar información a un profesional de los medios por parte de los poderes públicos puede constituir una interferencia lesiva del derecho a recibir y comunicar información consagrado en el art. 10 del Convenio, constituyendo un importante criterio a tomar en consideración para apreciar su efectiva vulneración "el hecho de que la información solicitada esté lista y disponible" (§ 169)"[10].

Es cierto que en diversos países de nuestro entorno se ha rehusado expresamente vincular el derecho de acceso configurado en la legislación de transparencia con el derecho fundamental a la libertad de información[11], o directamente se ha rechazado que los tribunales nacionales deban asumir la interpretación amplia del artículo 10 del Convenio adoptada en la STEDH *Magyar*[12]. Pero es igualmente cierto que nuestro propio texto constitucional impone un enfoque radicalmente diferente de la cuestión.

[9] Para más detalles sobre esta Sentencia, véanse Cotino Hueso (2017: 287-290) y Hernández Ramos (2019: 483-509).

[10] La doctrina *Magyar* es sistemáticamente empleada cuando hay ocasión para ello. Dejando a un margen las numerosas Decisiones que se fundamentan en la misma, baste mencionar las siguientes Sentencias: STEDH de 9 diciembre 2021, caso *Rovshan Hajivev/Azerbaijan*, en el que el solicitante de información era un periodista; STEDH de 1 de julio de 2021, caso *Association BURESTOP 55 y otros contra Francia*; STEDH de 3 de febrero de 2022. caso *Seks contra Croacia*, en el que la pretensión de información la formuló un investigador al objeto de hacer un libro.

[11] En este sentido, la Decisión de la Sala Primera del Tribunal Constitucional federal alemán de 20 de junio de 2017 -1 BvR 1978/13-.

[12] Véase la Sentencia, de 30 de julio de 2020, de la Upper Tribunal Administrative Appeals Chamber, caso D*erek Moss v the Information Commissioner and the Cabinet Office* (Appeal No: GIA/1531/2017).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

Así es; la incidencia de la jurisprudencia del TEDH tiene una virtualidad cualitativamente distinta para discernir la propia naturaleza de nuestro derecho de acceso a la información pública cuando se ejerce por los periodistas, habida cuenta de lo dispuesto en el art. 10.2 CE:

> "Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con… los tratados y acuerdos internacionales sobre las mismas materias ratificados por España".

Disposición según la cual –a juicio del Tribunal Constitucional- puede considerarse que es el contenido mismo de los derechos internacionalmente protegidos el que, en virtud de la interpretación, "se convierte en cierto modo en el contenido constitucionalmente declarado de los derechos y libertades que enuncia el capítulo segundo del título I de nuestra Constitución"(STC 36/1991, FJ 5º); hasta el punto de llegar a afirmarse que los reiterados Tratados configuran "de alguna manera el canon de constitucionalidad, aun cuando sin carácter autónomo"(STC 50/1995, FJ 4º). Y, como es obvio, la jurisprudencia constitucional ha vinculado específicamente ese mandato hermenéutico con el Convenio Europeo de Derechos Humanos: el artículo 10.2 de la Constitución -se afirma en la STC 341/1993, FJ 5º- "impone acudir a los tratados y acuerdos internacionales en la materia y, en particular, al ya citado Convenio de Roma, para interpretar el sentido y límites" de nuestros derechos fundamentales.

En suma, al ser "el Convenio europeo de derechos humanos […] un instrumento hermenéutico insoslayable para la interpretación de los derechos fundamentales de nuestra Constitución (art. 10.2 CE)"(STC 123/2005, FJ 3º), la jurisprudencia del TEDH que viene a delimitar el alcance del Convenio pasa a ocupar un papel esencial al respecto, como el propio Tribunal Constitucional no ha dudado reiteradas veces en reconocer: "Este Tribunal ha sido en todo momento consciente del valor que por virtud del art. 10.2 CE ha de reconocerse a la doctrina del Tribunal Europeo de Derechos Humanos en su interpretación y tutela de los derechos fundamentales"(STC 119/2001, FJ 6º)[13].

El puro y simple cumplimiento del mandato constitucional contenido en el artículo 10.2 CE no puede sino llevar a la conclusión de que, cuando es un periodista quien lo ejerce y se cumplen los requisitos fijados en la doctrina del TEDH, el derecho de acceso a la información pública muda de naturaleza y pasa a ser cualitativamente otra cosa. El acceso a la información pública, concebido con alcance general como

[13] Sobre la "particularidad hermenéutica" que supone el artículo 10.2 CE y el papel de la jurisprudencia del TEDH en la conformación de nuestros derechos fundamentales, consúltese Arzoz Santisteban (2014: 159-262).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.306

un derecho de configuración legal enraizado en el artículo 105 b) CE[14], pasa a operar, pues, en este supuesto, como el derecho fundamental consagrado en el artículo 20.1.d) CE. Y en consecuencia, de resultas de esta -por decirlo así- transustanciación, le resultan de plena aplicación los *tests* o estándares que ha ido perfilando la jurisprudencia constitucional en torno a la resolución de colisiones entre el derecho fundamental a la libertad de información con otros derechos o bienes jurídicos constitucionalmente protegidos.

Se trata de un enfoque que, aunque hasta el momento tan sólo haya sido asumido expresamente por contadas autoridades autonómicas de control de la transparencia[15], es únicamente una cuestión de tiempo que termine generalizándose, pues nadie pone en cuestión ni la aludida eficacia jurídica del art. 10.2 CE ni el alcance de la jurisprudencia acuñada por el TEDH sobre el particular.

Dicho esto, no podemos resistirnos a la tentación de reflexionar en voz alta acerca de si, acaso, no resulte contraproducente para facilitar la recepción en nuestro ordenamiento de esta jurisprudencia del TEDH la posición maximalista que sustenta que, siempre y en todo caso, el ejercicio del derecho de acceso a la información *ex* LTAIBG debe considerarse una proyección del derecho fundamental a la libertad de información consagrado en el artículo 20.1.d) CE.

Reflexión que, entre otras causas, ha sido aguijoneada por la reciente Sentencia del Tribunal Supremo 140/2023, de 7 de febrero (Recurso de casación nº 8005/2021), en donde la parte recurrente -que no era un periodista, sino "Greenpeace España"-, además del derecho de acceso de la LTAIBG, invocó el art. 20.1.d) CE y el artículo 10.1 del Convenio europeo. Enmarcada en términos genéricos la cuestión, el razonamiento del Tribunal Supremo tiene también un alcance general: "Se trata, por tanto -afirma refiriéndose al derecho de acceso derivado del artículo 105.b) CE-, de un derecho que no es un derecho fundamental, como se infiere de su configuración y ubicación sistemática en la Constitución, en el Título IV CE "del Gobierno y la Administración", y al margen, en definitiva, de la previsión del artículo 53.2 de la CE"(Fundamento de Derecho Cuarto). Y consecuentemente, dado que en el caso

[14] La STC 164/2021 ofrece la que constituye -hasta la fecha- la más detenida aproximación a la naturaleza jurídica del derecho de acceso: "El artículo 105 b) CE, encuadrado en el título IV, «Del Gobierno y de la Administración», incorpora un principio objetivo rector de la actuación de las administraciones públicas (artículo 103.1 CE), derivado de exigencias de democracia y transparencia, así como un derecho subjetivo de las personas, ejercitable frente a las administraciones, con sujetos, objeto y límites definidos en el propio precepto constitucional, que fue desarrollado inicialmente en los artículos 35 h) y 37 de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, y actualmente en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. […] A la vista de lo expuesto, debe señalarse que el acceso a la información integra el contenido de un derecho público subjetivo ejercitable frente a la administración que, no siendo absoluto, solo puede ser limitado por motivos predeterminados en la ley, en virtud de una previa ponderación de los intereses en juego. De este modo, la posibilidad de limitar el acceso a la información no constituye una potestad discrecional de la administración (FJ 1º.3)".

[15] Así, el Consejo de Transparencia y Protección de Datos de Andalucía ya se sumó a esta posición en la Resolución 10/2017 (FJ 2º). Véase asimismo la Resolución 330/2019 (FJ 6º).

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

enjuiciado no estaba en juego el ejercicio del derecho de acceso por un periodista, concluiría el Alto Tribunal que "la denegación de la solicitud de información pública a la recurrente sobre la exportación de morteros a Arabia Saudí no guarda relación alguna con el derecho a la libertad de información del artículo 20.1.d) de la CE" (Fundamento de Derecho Quinto) [16].

Parece evidente que las tajantes declaraciones arriba transcritas, si se extraen del contexto de la concreta controversia objeto de la decisión jurisdiccional, pueden ser utilizadas para respaldar la -errónea- tesis de que nunca ni en ningún caso el ejercicio del derecho de acceso configurado en la LTAIBG puede reconducirse al derecho fundamental a la libertad de información.

Sea como fuere, esta Sentencia del Tribunal Supremo no viene sino a ratificar la apreciación de que sería conveniente que se incorporara alguna referencia expresa al respecto en una hipotética futura modificación de la LTAIBG, puesto que serviría para hacer ver a todos los operadores jurídicos la exigencia constitucional de asumir esa comprensión del derecho de acceso como integrante del derecho fundamental a la libertad información cuando se ejercita con fines periodísticos. Pues, con independencia de si eso supondría materialmente en la práctica atribuir una posición más sólida a los periodistas que la ostentada por los restantes ciudadanos en los casos de colisión con el derecho a la protección de los datos personales (cuestión sobre la que no podemos ahora entrar), lo que resulta evidente es que el derecho de acceso de los periodistas así concebido sí pasa a disfrutar de los "privilegios jurisdiccionales" que, hoy por hoy, caracterizan a los derechos fundamentales consagrados en la Sección primera del Capítulo Segundo del Título Primero de la Constitución, a saber, ser tutelados mediante un procedimiento preferente y sumario y a través del recurso de amparo ante el Tribunal Constitucional (art. 53.2 CE).

4.- El artículo 15 LTAIBG en el contexto del RGPD

En el artículo 15 LTAIBG, el legislador afrontó la ardua tarea de trazar reglas, criterios y líneas directrices conforme a los cuales resolver los conflictos que inevitablemente surgen con el derecho a la protección de datos personales cuando se procede a la apertura generalizada de la información pública ante la ciudadanía. Tarea siempre necesaria para orientar a los operadores jurídicos, pero que adquiere un tinte particular en sistemas como el nuestro, en el que coexisten dos autoridades independientes de control que ejercen por separado sus competencias en sus respectivos ámbitos funcionales: la garantía de la transparencia y de la protección de los datos personales[17].

Naturalmente, no es este el lugar ni es la ocasión para realizar una incursión, siquiera somera, en el denso entramado de reglas, principios y criterios que conforman el

[16] Una primera aproximación crítica a esta Sentencia proporciona Blanes Climent (2023: *passim*).

[17] Salvando el caso del Consejo andaluz, que se configura como "autoridad independiente de control en materia de protección de datos y de transparencia en la Comunidad Autónoma de Andalucía" (artículo 43.1 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía).

CC BY SA

DOI: https://doi.org/10.51915/ret.306

artículo 15 LTAIBG. Nuestro objetivo es únicamente valorar su engarce en el nuevo marco normativo europeo, habida cuenta de que el RGPD ha entrañado cierto avance -aunque pueda fundadamente tildarse de "relativo"(Troncoso Reigada 2017: 997)- en la regulación del acceso a la información pública cuando entra en colisión con la protección de datos personales.

Aunque, muy probablemente, la principal transformación derivada de la entrada en vigor del RGPD resida en la propia naturaleza y función que desempeña el Reglamento en comparación con la derogada Directiva 95/46/CE. Si esta había jugado un muy significativo papel en la delimitación de nuestro derecho fundamental a la protección de datos personales en virtud del mandato hermenéutico establecido en el artículo 10.2 CE, el rol del RGPD deviene cualitativamente diferente y aún más relevante: al tratarse de un acto jurídico "obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro"(STC 76/2019, FJ 3º), toda controversia en la que se vea involucrado este derecho fundamental ha de sustanciarse y resolverse de acuerdo con lo dispuesto por el RGPD, de tal modo que el operador jurídico debe acordar la inaplicación de la normativa interna que lo contradiga. Sencillamente, la configuración de este derecho fundamental y su delimitación frente a otros derechos o bienes jurídicamente protegidos no corresponde ya en línea de principio a las Cortes Generales, sino al legislador europeo. Para decirlo con los gráficos términos utilizados por un antiguo director de la Agencia Española de Protección de Datos, con el RGPD se ha consumado "la abducción de un derecho constitucional convertido en un derecho exclusivamente europeo" (Rallo Lombarte 2019: 50).

Dicho sea más derechamente: las reglas y directrices establecidas en el artículo 15 LTAIBG sólo valen si y en la medida en que puedan compatibilizarse con la doctrina que vaya acuñando el Tribunal de Justicia de la Unión Europea al interpretar el RGPD.

Como es por todos conocido, el reiterado artículo 15 LTAIBG configura un régimen más o menos estricto de acceso a la información en función del mayor o menor nivel de protección del que disfruta el específico dato cuya divulgación se pretende. El máximo nivel de tutela se proporciona a las categorías especiales de datos mencionadas en el primer párrafo del artículo 15.1 LTAIBGD ("datos personales que revelen" la ideología, afiliación sindical, religión y creencias), toda vez que "el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso". Inmediatamente después en lo relativo a la intensidad de la garantía se encuentran los datos especialmente protegidos a los que se refiere el segundo párrafo del artículo 15.1 LTAIBG ("datos personales que hagan referencia" al origen racial, salud, vida sexual, datos genéticos o biométricos, así como los datos relativos a la comisión de infracciones penales o administrativas), ya que "el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley".

Estos datos cuya difusión se ve rodeada de particulares cautelas coinciden esencialmente con las categorías especiales de datos personales identificados en el

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

artículo 9.1 RGPD[18], salvando los datos concernientes a la comisión de infracciones, razón por la cual estos últimos serán objeto de un análisis específico más adelante.

Como hemos señalado líneas arriba, tanto la lectura del art. 15.1 LTAIBG como la aplicación de esas cualificadas categorías de datos personales a los casos concretos deben necesariamente ajustarse a las líneas jurisprudenciales que elabore el TJUE al interpretar el art. 9.1 RGPD. A este respecto, resulta sin duda de interés la Sentencia del Tribunal de Justicia (Gran Sala), de 1 de agosto de 2022 (asunto C-184/20), en donde resolvió una cuestión prejudicial sobre la normativa lituana que obliga a publicar en Internet los datos contenidos en las declaraciones de intereses privados de personas que trabajan como servidores públicos, así como de los directivos de asociaciones y establecimientos que reciben fondos públicos. Los datos de las declaraciones que se publicaron no hacían ninguna referencia explícita -claro está- a la orientación sexual de los declarantes, pero las declaraciones sí podían contener información sobre personas identificables con las que aquellos estaban en relaciones o con las que cohabitaban. ¿Cabe considerar que esta información aporta "datos relativos" a la orientación sexual, y por tanto entenderse que se encuentran bajo el ámbito de cobertura del art. 9.1 RGPD? O para decirlo con la más atinada formulación empleada por el Tribunal, la cuestión a resolver residía en "determinar 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). Y la respuesta de la Gran Sala fue que "el tratamiento de datos personales que puedan desvelar indirectamente informaciones sensibles sobre una persona física" no queda extramuros del régimen de protección reforzado establecido en el 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). Obviamente, esta pauta interpretativa debe tenerse muy presente cuando se proceda a la aplicación del artículo 15.1 LTAIBG como límite del derecho de acceso o de la publicidad activa.

En contraste con este reforzado régimen de tutela del que gozan los datos identificados en el art. 15.1 LTAIBG, cuando se trata de "datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano", el legislador optó por consagrar una regla general de prevalencia a favor del derecho de acceso (art. 15.2 LTAIBG).

Pero entre el espacio ocupado por los datos especialmente protegidos y el espacio reservado a los datos meramente identificativos se extiende un ancho campo en el que tienden a concentrarse las controversias. A su elucidación el legislador dedicó el tercer apartado del art. 15 LTAIBG.

[18] "Quedan prohibidos -dice el art. 9.1. RGPD- el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

4.1.- Los criterios de ponderación del apartado tercero del artículo 15 LTAIBG

Efectivamente, en los restantes casos en que no entran en juego los datos previamente mencionados en el artículo 15, habrá que proceder de acuerdo con lo dispuesto en su apartado tercero, a saber, la Administración interpelada "concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal". Y añade el precepto a continuación cuatro criterios que la Administración "tomará particularmente en consideración" para efectuar tal ponderación.

Muy pronto un autorizado sector de la doctrina vertió severas críticas sobre la regulación de tales criterios, señaladamente en relación con los dos primeros[19] (baste mencionar Fernández Ramos y Pérez Monguió 2017: 219-221; Guichot Reina 2014: 137-139; Troncoso Reigada 2017: 1015-1022). A mi juicio, aún parece más reprochable la omisión de un criterio que, lisa y llanamente, es determinante en nuestra jurisprudencia constitucional (y en la de los países de nuestro entorno) para la resolución de las controversias entre la libertad de información y los derechos al honor, intimidad y a la propia imagen (art. 18.1 CE), y que obviamente podía y debía proyectarse al derecho fundamental a la protección de datos personales, a saber, presumir la pertinencia de conceder el acceso cuando los datos versen sobre personas que desempeñen cargos o funciones públicas en relación con el desempeño de su actividad. Ausencia tanto más sentida cuanto que la incorporación de este criterio fue sugerida por el entonces director de la Agencia Española de Protección de Datos durante su comparecencia en la Comisión Constitucional del Congreso de los Diputados[20].

Es cierto que el listado de criterios recogido en el art. 15.3 LTAIBG no tiene un carácter exhaustivo, de tal modo que pueden emplearse cualesquiera otros que se consideren pertinentes al objeto de resolver la ponderación; y de hecho algunas de las autoridades independientes de control, desde el arranque mismo de su actividad[21], utilizaron con plena naturalidad la doctrina constitucional sobre la condición pública o privada de la persona involucrada para fundamentar sus decisiones. Pero no es menos verdad que su inclusión expresa en la LTAIBG habría facilitado sin duda la tarea al personal encargado

[19] "a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos".

[20] Tomo la referencia de Guichot Reina (2014: 127).

[21] Así, por ejemplo, véase la Consulta 1/2016, de 11 de mayo, del Consejo de Transparencia y Protección de Datos de Andalucía (Consideración Jurídica tercera).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.306

en las diversas Administraciones de atender las solicitudes de información, habida cuenta de la complejidad técnica inherente a la articulación de los juicios de ponderación[22].

Comoquiera que sea, la utilización de este criterio y su adecuada valoración en el curso de la ponderación pueden considerarse exigencias impuestas por el propio TJUE en caso de colisión entre la difusión de la información y el derecho a la protección de datos personales cuando de medidas contra la corrupción se trata. Así se desprende de la arriba citada Sentencia del Tribunal de Justicia (Gran Sala), de 1 de agosto de 2022, en donde además se añaden algunas precisiones para alcanzar un "ajuste fino" en la resolución del conflicto: "[…] a efectos de esta ponderación debe tenerse en cuenta, en particular, la circunstancia de que el interés general en que se publiquen datos personales puede variar con arreglo a la importancia de las funciones ejercidas por el declarante, especialmente, su posición jerárquica, la extensión de las competencias de administración pública que tenga atribuidas, en su caso, y los poderes de que dispone en materia de compromiso y gestión de fondos públicos"(apartado 111; en la misma línea, el apartado 86).

No estaría de más que en un renovado texto de la LTAIBG se incorporaran explícitamente consideraciones de esta índole u otras semejantes en el listado de criterios orientadores de la ponderación.

4.2.- El acceso a la información relativa a infracciones administrativas

El RGPD también ha introducido alguna modificación reseñable en la regulación que hacía la Directiva 95/46/CE del tratamiento de datos relativos a infracciones administrativas. En el artículo 8 de la Directiva -dedicado al "Tratamiento de categorías especiales de datos"- se incluía un quinto apartado cuyo objetivo era regular el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, estableciendo como regla general que el mismo sólo podría realizarse bajo el control de la autoridad pública; pero dicho apartado quinto terminaba

[22] Complejidad que naturalmente no pasó inadvertida al legislador como lo atestigua la Disposición adicional quinta de la LTAIBG, al establecer que el Consejo de Transparencia estatal y la Agencia Española de Protección de Datos "adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma…" (sobre esta disposición, consúltese Rodríguez Álvarez 2016: 81-85). Por lo demás, la dificultad de trazar en abstracto nuevas pautas generales que perfilen las reglas establecidas en el art. 15 LTAIBG quizá explique lo reducido del número de Criterios Interpretativos conjuntos aprobados hasta la fecha.

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

abriendo a los Estados la posibilidad de que extendieran tal exigencia al tratamiento de datos concernientes a sanciones administrativas[23].

Posibilidad de la que, en efecto, haría uso el legislador español al elevar, en la LO 15/1999 reguladora de los datos personales, el tratamiento de los datos atinentes a las infracciones administrativas al mismo nivel de protección que el dispensado a los datos relativos a las infracciones de carácter penal[24]. Alzados, así, los datos relativos a infracciones administrativas a la condición de "datos especialmente protegidos" en virtud de la decisión del legislador orgánico, la LTAIBG estableció idéntica protección a estos datos que a los concernientes a las infracciones penales: "Si la información incluyese […] datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley"(segundo párrafo del artículo 15.1).

Se trataba, ciertamente, de una decisión acorde con las previsiones de la LOPD de 1999, pero que recibió numerosas críticas desde el punto de vista de la transparencia, habida cuenta de que suponía opacar un entero sector de la realidad (procedimientos administrativos sancionadores, incluyendo las sanciones disciplinarias) muy relevante para asegurar una eficaz supervisión de la gestión de la cosa pública por parte de la ciudadanía[25]. Sea como fuere, dados los inequívocos términos del art. 15.1 LTAIBG, las autoridades independientes de control de la transparencia se encontraron, pues, con el pie forzado de aplicar la regla en cuestión y, en consecuencia, con la obligación de denegar el acceso cuando no se contase

[23] El tenor literal del art. 8.5 de la Directiva era el siguiente: "El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos".

[24] En efecto, en el apartado quinto de su art. 7 -artículo donde se aborda la regulación de los "datos especialmente protegidos"- se situaban ambas categorías de datos en el mismo plano: "Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras".

[25] Baste citar: Fernández Ramos y Pérez Monguió (2017: 205-208) y Guichot Reina y Barrero Rodríguez (2020: 423-425). Sencillamente, el grueso de la mejor doctrina entendía que "no se debería excluir *a priori* la ponderación por el órgano administrativo tampoco en estos supuestos, ya que hay casos concretos en los que existe un interés legítimo que puede justificar el acceso" (Troncoso Reigada 2017: 1044).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.306

con el consentimiento del afectado, pese a la manifiesta relevancia pública que pudiera tener la información pretendida[26].

Pero, como decía, el RGPD ha introducido algún cambio significativo en la regulación de esta cuestión respecto de la Directiva 95/46/CE. En primer lugar, los propios datos concernientes a infracciones penales, aun conservando un estatus singular, ya no se conectan con las "categorías especiales de datos personales" que el artículo 9 RGPD se encarga de delimitar. Ahora, se desplaza su regulación al artículo 10 RGPD, que se circunscribe exclusivamente al "Tratamiento de datos personales relativos a condenas e infracciones penales"[27]. Y por otro lado, y sobre todo, el RGPD a diferencia de la Directiva no hace ninguna referencia explícita al tratamiento de datos concernientes a infracciones administrativas.

Con base en el tenor literal del artículo 10 RGPD y apoyándose asimismo en el proceso de elaboración del precepto, el TJUE ha declarado en términos categóricos que el mismo limita "al ámbito penal la mayor protección prevista en esta disposición" [Sentencia del Tribunal de Justicia (Gran Sala), de 22 de junio de 2021, asunto C-439/19 (*Puntos de penalización*), especialmente apartados 77 y 78][28].

En este nuevo marco normativo trazado por el RGPD, salta a la vista que resultaba muy difícil de justificar el mantenimiento de la equiparación entre el acceso a los datos sobre infracciones administrativas y las categorías especiales de datos (en esta línea, Guichot Reina 2018: 67-68), destacándose que dicha equiparación podía generar zonas de conflicto con la transparencia

[26] Por lo que no dejó de deslizarse alguna velada crítica a esta visión capitidisminuida de la transparencia que había hecho suya el legislador: "Comoquiera que sea, con independencia de la valoración que merezca la decisión del legislador de estrechar el derecho a saber de la ciudadanía cuando se pretende acceder a datos de personas físicas relativos a la comisión de infracciones administrativas, lo cierto es que este Consejo no encuentra nada que reprochar a la Resolución denegatoria a la luz del citado artículo 15.1 LTAIBG. En efecto, dado que no consta el consentimiento expreso de la persona objeto del procedimiento disciplinario ni su acceso está amparado por norma con rango legal, no procede sino desestimar la presente reclamación" (Resolución del Consejo de Transparencia y Protección de Datos de Andalucía 435/2018, FJ 3.º).

[27] El citado artículo 10 RGPD dice así: "El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas."

[28] En cualquier caso, debe notarse que, según afirma esta Sentencia en su apartado 85, "el concepto de «infracción penal», decisivo para determinar la aplicabilidad del artículo 10 del RGPD [a los datos personales relativos a infracciones de tráfico como las controvertidas en el litigio principal], requiere, en toda la Unión, una interpretación autónoma y uniforme, que debe buscarse teniendo en cuenta el objetivo que pretende alcanzar dicha disposición y el contexto en que esta se incluye, sin que sea determinante a este respecto la calificación dada por el Estado miembro de que se trate a esas infracciones, calificación que puede ser diferente de un país a otro…"

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

o con el propio desarrollo de la administración electrónica (Jiménez Asensio 2019: 110-111).

Y, ciertamente, no cabe sino afirmar que el legislador orgánico ha sido sensible a la conveniencia de adecuar el régimen de transparencia a este nuevo escenario jurídico. En efecto, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), ha optado por dedicar a la regulación de esta materia el artículo 27, que se halla en el Título IV ("Disposiciones aplicables a tratamientos concretos").

Según dispone el apartado primero de este art. 27 LOPDGDD:

> "A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá: a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones. b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquél".

Y prosigue estableciendo el segundo apartado del artículo que nos ocupa:

> "Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a instrucciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados".

Como es palmario, la LOPDGDD parte de un enfoque sustancialmente diferente al vigente hasta la fecha de su aprobación, toda vez que la exigencia del consentimiento del afectado únicamente opera en el supuesto de que el acceso a los datos sobre infracciones administrativas no sea acordado por el órgano competente en la materia, o bien si la decisión de este no se circunscribe a los datos estrictamente necesarios para alcanzar la finalidad perseguida con el pretendido acceso a la correspondiente información.

Que el principal objetivo del legislador orgánico no fue otro que flexibilizar el régimen de acceso a este tipo de datos personales, es una conclusión que se hizo evidente desde el arranque mismo del procedimiento legislativo. Ya en el Anteproyecto de la Ley Orgánica aparecía esta disposición en una redacción próxima a la definitivamente aprobada, aunque se ubicaba como artículo 4 en el comienzo del Título II –"Principios de protección de datos"-, puesto que fundamentaba su regulación, no en el artículo 86 RGPD, sino en el artículo 5.1.c) RGPD (principio de minimización de datos). Sin embargo, según argumentó persuasivamente el Consejo de Estado, del art. 5.1.c) RGPD no cabía inferir ninguna capacidad de los Estados miembros para proceder a su desarrollo o concretización; razón por la cual sugirió el art. 86 RGPD como base que apuntalase la facultad del legislador de someter el tratamiento de este tipo de datos a condiciones

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
El conflicto entre la transparencia y la protección de datos…
por Manuel Medina Guerrero
Págs. 51-73
DOI: https://doi.org/10.51915/ret.306

específicas[29]. Y, consecuentemente, propuso el traslado del entonces artículo 4 al Título IV de la Ley Orgánica; sugerencias que, como ya sabemos, terminarían plasmándose en el texto definitivo de la LOPDGDD.

Así, pues, tal y como expresa su propio tenor literal, con el art. 27 LOPDGDD[30] el legislador no vino sino a hacer uso en la práctica de la cláusula de apertura facultativa que habilita a los Estados miembros para conciliar el derecho a la protección de datos personales con el acceso a los documentos oficiales (art. 86 RGPD).

Pese a ello, la actual redacción del artículo 15.1 LTAIBG -aunque fue modificada por la Disposición final undécima de la propia LOPDGDD- sigue manteniendo en idénticos términos que la versión inicial la tutela conferida a los "datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor", de tal modo que el acceso a dicha información "sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley".

En suma, nos encontramos con la paradoja de que la misma Ley Orgánica que da una nueva redacción al artículo 15.1 LTAIBG (Disposición final undécima), pero preserva el mismo régimen que su versión inicial exigiendo el consentimiento del afectado para permitir el acceso a datos relativos a infracciones administrativas, adopta en su artículo 27 una regulación más proclive a la transparencia por cuanto la exigencia del consentimiento únicamente opera de forma subsidiaria, a falta del cumplimiento de alguno de los requisitos antes referidos. Nos hallamos, pues, ante una evidente contradicción entre el art. 27 LOPDGDD y el art. 15.1 LTAIBG, que obviamente ha de resolverse por vía interpretativa dando preferencia al régimen establecido por el primero. Aunque, como no es menos obvio, en aras de la seguridad jurídica, sería más que conveniente que en una hipotética futura reforma de la LTAIBG el tenor literal de su artículo 15.1 se acomodara expresamente a lo dispuesto en la LOPDGDD.

5.-La LTAIBG como ley parcialmente orgánica

Como adelantamos al comienzo de estas páginas, cabe fundadamente dudar de que la inclusión del artículo 15 en una Ley aprobada en su totalidad como ordinaria respetase lo previsto en el art. 81.1 CE, que incluye entre las leyes orgánicas a "las relativas al desarrollo de los derechos fundamentales y de las libertades públicas". Pues, de acuerdo con la consolidada jurisprudencia del Tribunal Constitucional, "lo

[29] Apelación al art. 86 RGPD que efectúa el Consejo de Estado tras hacerse eco de la respuesta de la AEPD a la carta de la Comisión de fecha 9 de agosto de 2017, en donde alegaba que "el acceso a este tipo de datos está prohibido en Derecho español por el artículo 15.2 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que prevé que sólo cabrá en los supuestos previstos en una norma con rango de Ley o previo consentimiento del interesado, lo que en consecuencia impide el tratamiento de dichos datos a menos que concurran esas mismas condiciones" [Dictamen del Consejo de Estado, de 26 de octubre de 2017, sobre el anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal (número de expediente: 757/2017)].

[30] Para un análisis más detallado de este artículo, consúltese Cubero Marco (2021: *passim*).

CC BY SA

DOI: https://doi.org/10.51915/ret.306

que está constitucionalmente reservado a la Ley Orgánica es la regulación de determinados aspectos esenciales para la definición del derecho, la previsión de su ámbito y la fijación de sus límites en relación con otras libertades constitucionalmente protegidas" (baste citar la STC 135/2006, FJ 2º). En suma, el establecimiento de restricciones o límites a los derechos fundamentales constituye un asunto reservado al legislador orgánico (SSTC 101/1991, FJ 2º; 127/1994, FJ 4º; 88/1995, FJ 4º; 173/1998, FJ 7º).[31] Y parece evidente que el artículo 15 LTAIBG no viene sino a regular los límites del derecho fundamental a la protección de datos personales frente al derecho de acceso a la información pública, concebido como derecho público subjetivo anclado en el art. 105.b) CE (en este sentido, la arriba citada STC 164/2021, FJ 1.3).

En lo concerniente a la limitación del derecho a la protección de datos personales en relación con el derecho de acceso a información que contiene datos especialmente protegidos, la versión originaria del apartado primero del art. 15 LTAIBG se fundamentaba expresamente en las reglas establecidas en los apartados segundo y tercero del art. 7 de la entonces vigente Ley Orgánica reguladora del derecho a la protección de datos de carácter personal (LO 15/1999), lo que obviamente excluía considerar que el legislador ordinaria usurpase en este concreto ámbito una tarea reservada al legislador orgánico. Pero la cuestión distaba mucho de estar tan clara en las otras limitaciones del derecho fundamental *ex* art. 18.4 CE previstas en el art. 15 LTAIBG. Así, no era nada fácil hallar un específico anclaje en la LO 15/1999 de la regla de preferencia a favor del derecho de acceso a la información contenida en el apartado segundo del tantas veces citado art. 15 LTAIBG (datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano). Y otro tanto cabía decir de su apartado tercero, el cual, respecto de la información que no contenga datos especialmente protegidos, determina que la Administración "concederá el acceso previa ponderación"[32], enumerando a continuación unos criterios que deberán tomarse "particularmente en consideración" al ponderar.

Por su parte, la actual LOPDGDD tampoco ha incorporado a su articulado un anclaje específico relacionado con las referidas limitaciones. Es más, no contiene ningún precepto semejante a los apartados segundo y tercero del art. 7 de la derogada LO 15/1999, por lo que su entrada en vigor podía incluso acrecentar las dudas acerca de la insuficiencia de rango del art. 15 LTAIBG.

Pues bien, según parece, este problema no pasó inadvertido al legislador orgánico, aunque -de ser así- no puede ciertamente afirmarse que lo haya solventado con la debida claridad. Es verdad que la Disposición final primera LOPDGDD atribuye rango

[31] Consúltese Sala Sánchez (2018: 194-196) para un examen más detallado de la jurisprudencia constitucional recaída sobre las leyes orgánicas de desarrollo de derechos fundamentales y libertades públicas.

[32] Formulación que ha permitido llegar a la conclusión de que el precepto "recoge veladamente un principio general *pro acceso*" (Troncoso 2017: 1010).

DOI: https://doi.org/10.51915/ret.306

de ley orgánica a la Disposición adicional segunda[33], que recuerda en los siguientes términos la aplicabilidad de la LTAIBG cuando la transparencia afecte a datos de carácter personal:

"La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica".

¿Supone esto que se estén invistiendo del carácter de orgánico a los artículos 5.3 y 15 LTAIBG? Si esta era la voluntad del legislador, habría resultado tanto más esclarecedor que se hubiese llevado explícitamente este reconocimiento a la modificación de la LTAIBG acometida en la Disposición final undécima de la LOPDGDD. Sea como fuere, resultaría en todo caso conveniente que la referencia expresa a su carácter orgánico se incorporase en una futura reforma de la LTAIBG.

[33] También atribuye carácter orgánico a la Disposición adicional decimoséptima, en donde se enumeran diferentes leyes ordinarias que regulan el tratamiento de datos relacionados con la salud.

CC BY SA

DOI: https://doi.org/10.51915/ret.306

Bibliografía

ARZOZ SANTISTEBAN, X. 2014. *La concretización y actualización de los derechos fundamentales*, Madrid: CEPC.

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).

BUCHNER, B. y TINNEFELD, M. D. 2018. "Comentario al artículo 85", en KÜHLING, J. y BUCHNER, B. (Hrsg.), *Datenschutz-Grundverordung/Bundesdatenschutzgesetz* (Kühling/Buchner, Hrsg.), 2. Auflage, München: C.H. Beck, pp. 1157- 1166.

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

CUBERO MARCO, J. I. 2021. "Tratamiento de datos relativos a infracciones y sanciones administrativas (Comentario al artículo 27 LOPDGDD)", en TRONCOSO REIGADA, A. (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo II, Cizur Menor: Civitas/Thomson Reuters, pp. 3823-3854.

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

FERNÁNDEZ RODRÍGUEZ, J. J. 2021, "Tratamiento y libertad de expresión y de información (comentario al artículo 85 RGPD)", en TRONCOSO REIGADA, A. (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo II, Cizur Menor: Civitas/Thomson Reuters, pp. 3303-3312.

GUICHOT REINA, E. 2014. "Capítulo IV. Límites a la transparencia y el acceso a la información", en GUICHOT, E. (coord.), *Transparencia, Acceso a la Información Pública y Buen Gobierno*, Madrid: Tecnos/Instituto García Oviedo, pp. 97-142.

GUICHOT REINA, E. 2018. "El acceso a los datos referidos a expedientes sancionadores o disciplinarios a la luz de la nueva normativa sobre protección de datos", *Revista Española de la Transparencia*, núm. 6: 65-72.

GUICHOT, E. y BARRERO RODRÍGUEZ, C. 2020. *El derecho de acceso a la información pública*, Valencia: Tirant lo Blanch.

HERBST, T. 2018, "Comentario al artículo 86", en KÜHLING, J. y BUCHNER, B. (Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz. Kommentar*, 2. Auflage, München: C. H. Beck, pp. 1166-1171.

HERNÁNDEZ RAMOS, M. 2019. "El derecho de acceso a la información pública en la jurisprudencia del Tribunal Europeo de Derechos Humanos: un derecho

CC BY SA

instrumental imprescindible para la eficacia del Convenio desde la teoría general de los derechos". *Teoría y Realidad Constitucional*, núm. 42: 483-509.

JIMÉNEZ ASENSIO, R. 2019. *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*, Oñati: IVAP.

KRANENBORG, H. 2020, "Comentario al art. 86", en KUNER, C. Y BYGRAVE, L. Y DOCKSEY, C. (ed.), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford: Oxford University Press, pp. 1213-1222.

KÜHLING, J. *et al.* 2016, *Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf*, Münster: Verlagshaus Monsenstein und Vannerdat OHG.

PAULY, D. A. 2021. "Comentario al artículo 86", en PAAL, B. P. y PAULY, D. A. (Hrsg.), *Datenschutz-Grundverordnung. Bundesdatenschutzagesetz*, München: C. H. Beck, pp. 1078-1081.

RALLO LOMBARTE, A. 2019. "El nuevo derecho de protección de datos", *Revista Española de Derecho Constitucional*, núm. 116: 45-74.

RODRÍGUEZ ÁLVAREZ, J. L. 2016. "Transparencia y protección de datos: criterios legales de conciliación", en CANALS AMETLLER (ed.), Dolors Canals Ametller (ed.): *Datos. Protección, Transparencia y Buena Regulación*, Girona: Documenta Universitaria, Girona, 2016, pp. 53-85.

SALA SÁNCHEZ, P. 2018. "Comentario al artículo 81", en RODRÍGUEZ-PIÑERO Y BRAVO FERRER, M. y CASAS BAAMONDE, M. E. (directores): *Comentarios a la Constitución Española*, Tomo II, Madrid: Fundación Wolters Kluwer/BOE/Tribunal Constitucional/Ministerio de Justicia, pp. 181.

SPECHT, L. y BIENEMANN, L. 2018. "Comentario al artículo 86", en SYDOW, G. (Hrsg.), *Europäische Datenschutzgrundverordnung. Handkommentar*, Baden-Baden: Nomos, pp. 1455-1464.

TRONCOSO REIGADA, A. 2017. "La protección de datos personales como límite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 'Protección de datos personales'", en TRONCOSO REIGADA, A. (dir.), *Comentario a la Ley de transparencia, acceso a la información pública y buen gobierno*, Cizur Menor: Aranzadi/Thomson Reuters, pp. 959-1079.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

Elecciones, protección de datos y transparencia en la publicidad política: la apuesta normativa de la UE y sus efectos en el ordenamiento español

Rosario García Mahamut[1]

Catedrática de Derecho Constitucional
Universidad Jaume I de Castellón

España

ORCID: 0000-0002-7602-8136

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

Este trabajo se ha realizado en el marco del proyecto del Ministerio de Ciencia e Innovación DATATRANSCO (Referencia: PID 2021-128309NB-I00).

RESUMEN: Garantizar la integridad de las elecciones constituye un objetivo prioritario de los Estados democráticos. Las elecciones en el mundo digitalizado evidencian un elenco interminable de amenazas cuyo epicentro parte de la datificación y del uso de herramientas y técnicas al servicio de la manipulación de la voluntad política. La exigencia de transparencia, y la definición de sus requisitos, para los proveedores de la publicidad política, así como la prohibición de técnicas de segmentación de este tipo de publicidad especialmente durante la campaña electoral constituyen un deber jurídico inaplazable para el legislador nacional y europeo. De ahí que en este trabajo se analice la propuesta de la Comisión del Reglamento del Parlamento Europeo y del Consejo sobre la transparencia y la segmentación política, tras la fijación de posición del Parlamento Europeo (febrero 2023), y se reflexione sobre algunas de sus implicaciones y efectos en la normativa electoral española.

[1] Catedrática de Derecho Constitucional de la Universitat Jaume I de Castellón. Coordinadora del Grupo de Investigación Protección de Datos y Derechos Fundamentales (PRODADEF). Investigadora principal de varios proyectos de investigación nacionales sobre protección de datos e investigadora en diversos proyectos de investigación europeos sobre la materia. Autora de numerosos libros, artículos y capítulos de libros de difusión internacional.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

PALABRAS CLAVE: Elecciones, transparencia y protección de datos; publicidad política; manipulación y desinformación en campaña electoral; técnicas de microsegmentación; elecciones Parlamento Europeo.

CONTENIDOS: 1.-El contexto de partida. 2.-La integridad de las elecciones en el entorno digital: una visión holística del binomio protección de datos y exigencia de transparencia en la publicidad política. 3.-La propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la transparencia y la segmentación de la publicidad política: Principales objetivos. 4.-Una visión de conjunto de las enmiendas aprobadas por el Parlamento Europeo: La apuesta por garantizar la transparencia y la protección de datos. 5.- Una aproximación sobre los efectos del Reglamento de transparencia en el régimen electoral español. 6.-Reflexiones conclusivas. - Bibliografía.

Elections, data protection and transparency in political advertising: the EU regulatory commitment and its effects on the Spanish legal system

ABSTRACT: Guaranteeing the integrity of the elections constitutes a prioritized objective of democratic States. Elections in the digitized world reveal an endless list of threats and its epicenter stems from datafication and the use of tools and techniques at the service of manipulating political will. The obligation of transparency, and the definition of its requirements for providers of political advertising, as well as the prohibition of segmentation techniques for this type of advertising, especially during the electoral campaign, represent a legal duty that cannot be postponed for the national and European legislator. Hence, this paper analyses the Commission proposal for a regulation of the European Parliament and the Council transparency and political segmentation, after the establishment of the position of the European Parliament (February 2023) with the aim to reflect on some of its implications and effects on the Spanish electoral regulations.

KEYWORDS: Elections, transparency and data protection; political advertising; manipulation and misinformation in the electoral campaign; microsegmentation techniques; elections to the European Parliament.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

1.- El contexto de partida

Defender los procesos democráticos es sinónimo de combatir el fraude y los intentos deliberados de manipular las elecciones. En el modelo de campaña electoral tradicional, "fuera de línea", la aplicación de las reglas del proceso electoral ha permitido el desarrollo de campañas políticas que han ofrecido a los electores una visión amplia sobre los programas e ideas de los partidos que concurren a las elecciones; sin embargo, no podemos decir lo mismo de las campañas que se desarrollan en el entorno digital y que amenazan gravemente la integridad del proceso electoral sobre las que se ciernen y proyectan una pléyade de graves amenazas sobre la integridad del proceso electoral.

La especial relevancia que la protección de los datos personales adquiere en el contexto electoral resulta del todo punto indiscutible[2]. Todos los aspectos tecnológicos, económicos, jurídicos y de políticas públicas, entre otros, que se diseñen y ejecuten para la salvaguarda del uso y tratamiento *legítimo* de los datos personales en el entorno digital constituyen la clave de bóveda sobre la que descansa la *alma mater* de unas elecciones libres en un Estado Democrático.

En este contexto, el uso masivo y el tratamiento *ilegítimo* de los datos personales no solo son susceptibles de vulnerar los derechos subjetivos de las personas a la protección de sus datos, o las de las reglas del juego en la confrontación política que garantiza el derecho fundamental de sufragio activo y pasivo (art. 23 CE). Más allá de cualquier derecho subjetivo en juego conculcado, los datos personales —directamente recogidos, observados o inferidos— constituyen el centro neurálgico sobre el que orbita la mayor parte de las amenazas que ponen en jaque un principio tan esencial para la existencia misma del sistema democrático como el de garantizar la integridad de las elecciones en el actual contexto digital[3] con nuevas técnicas y aplicaciones de inteligencia artificial.

Los riesgos no vienen por los avances tecnológicos, o no vienen exclusivamente por el uso de herramientas tecnológicas que avanzan al tiempo del segundero del reloj.

[2] Algunas de estas cuestiones ya las abordé en su momento cuando apenas existían estudios en nuestro ordenamiento (Cfr. García Mahamut 2015 a): 481- 512 y 2015 b): 309-338). Sobre el particular remitimos entre otros a la contribución de la Comisión Europea en el Documento de "Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral" COM (2018) 638 final, 12.9.218 y la Declaración del CEPD 2/2019 sobre el uso de datos personales durante las campañas políticas, 13.3. 2019.

[3] Remitimos, entre otros y además de los trabajos anteriormente citados, a Arenas Ramiro, M. (2019: 341-372); García Sanz, R.M., (2019: 129-159) o Hernández Peña J.C., (2022: 41- 73).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

Es, en sí misma, "la datificación" y su explotación —*data driven campaign*— la condición *sine qua non* para la manipulación de la información y del engaño a gran escala en la confrontación política[4]. No cabe obviar, bajo ninguna hipótesis de trabajo rigurosa, que la inteligencia artificial ya está en todas partes y, utilizando expresión del presidente de la FRA Michael O'Flaherty, "afecta a todos, desde nuestras redes sociales hasta los beneficios sociales que recibimos"[5].

Los datos personales de cada uno de los electores constituyen el arma más poderosa sobre los que obtener una información que se perfila y se personaliza para luego redirigírsela con objetivos espurios en un contexto de marcada confrontación política[6] en la que los ciudadanos deben formarse una opinión sobre las propuestas que los distintos partidos políticos ofrecen y defienden para votar por alguna de ellas.

Un escenario real y jurídico desolador cuando las redes sociales y las nuevas tecnologías se utilizan para difundir a gran escala, aunque se dirija de forma personalizada, campañas de desinformación y manipulación con un rasgo definidor: generar un amplísimo efecto eco (caja de resonancia) en el resto de los electores[7]. No tienen nada de ingenuo los objetivos que persiguen la explotación de los datos cuando, por ejemplo, el resultado de unas elecciones se puede decantar por un estrechísimo margen de votos; o cuando de por sí son los intereses propios de otros países y gobiernos los que mueven los hilos de los cambios de gobierno de otro país, amén, obviamente, de los concretos ciberataques o amenazas híbridas.

---

[4] No obstante, convenimos con G. Kefford, K Dommett y E. Rzepecki (2022) que los partidos políticos dependiendo del contexto pueden carecer de la capacidad para ejecutar prácticas muy incisivas asociadas con las campañas basadas en datos.

[5] Bias in algorithms. Artificial Intelligence and discrimination, Report, FRA, 2022: 3., doi:10.2811/25847.

[6] Si bien, algunos estudios en nuestro país cuestionan los auténticos efectos reales que ello pudiera tener sobre los ciudadanos. En ese sentido remitimos por todos al trabajo de Hernández Peña J.C., (2022: 71-73) y a la bibliografía allí citada. Sin ánimo de realizar una exhaustiva alusión de los estudios que tratan de cuantificar los efectos del uso de Internet en los modelos de comunicación política o en la organización de los partidos en distintos sistemas, remitimos, entre otros, a los trabajos de Latimer, Ch.P., (2008: 81-95) o R. Gibson & S. Ward., (2009: 87-100),

[7] Naturalmente, independientemente de que "la difusión de desinformación y de narraciones polarizadas puede agravar las divisiones y los conflictos de la sociedad" utilizando expresión recogida en las conclusiones de la 17ª Conferencia Europea de los órganos encargados de la administración electoral "El derecho electoral y la administración electoral en Europa desafíos recurrentes y buenas prácticas", celebrada el 12 y 13 de noviembre de 2020, Comisión de Venecia, CDL-PI (2020)017, p.3.(https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2020)017-spa).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

La campaña electoral es una de las fases del proceso en el que la manipulación de los electores puede tener un impacto directo sobre su conducta ante las urnas. Es justamente en ese espacio de tiempo en el que los contendientes en liza tratan de convencer al electorado de que son "su" mejor opción política para continuar en el Gobierno o convertirse en alternativa del Gobierno. A modo de trazo grueso, es básicamente esa fase del proceso en la que los electores sopesan las distintas alternativas y programas políticos de quienes concurren a las elecciones, ultiman su decisión sobre cuál es el partido y/o candidato que va a defender el programa de gobierno que más se adecúe a sus creencias y opiniones y, tras el día de reflexión como exige la LOREG en nuestro ordenamiento, expresar a través de su voto su preferencia política sobre quién debe gobernar el país.

Reforzar normativamente todas las medidas y herramientas que garanticen durante la campaña que todos los actores e intermediarios (incluidos los proveedores de servicios y los servicios conexos) cumplan con los requisitos de transparencia en todos los frentes (tecnológicos, algorítmicos, publicitarios, económicos…) constituye un deber jurídico inexcusable de los poderes públicos para controlar y evitar la manipulación, el engaño y la desinformación de los electores.

En las campañas en línea[8] los controles jurídicos se muestran débiles ante la difuminación de las líneas divisorias que permiten distinguir la información de la publicidad política engañosa, o dicho de otro modo la información y la desinformación volitiva[9].

De ahí que definir y garantizar los requisitos de transparencia en la actuación de la pluralidad de actores públicos y privados en el proceso electoral constituye un elemento absolutamente esencial para evitar la manipulación y el engaño a gran escala. Obsérvese que lo que se pone en entredicho, como ya advertí en un trabajo anterior[10], es la propia capacidad del proceso electoral para desempeñar su papel fundamental de legitimar al poder político.

Dada la imposibilidad de abordar todos y cada uno de los elementos que afectan a los requisitos de la transparencia del proceso electoral en el contexto digital, me ceñiré a abordar uno de sus aspectos más relevantes: el de la formación de la opinión pública y el tratamiento normativo sobre la publicidad política que se contempla en la propuesta de Reglamento adoptada por la Comisión Europea sobre la

[8] Para obtener una visión de conjunto en nuestro ordenamiento remitimos a Sánchez Muñoz, O. (2020).

[9] Sobre algunas de estas cuestiones, véase Serra Cristóbal, R., (2023: 13-46).

[10] García Mahamut, R. (2015 a): 512).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

transparencia y la segmentación de la publicidad política (PRTSP) cuyo objetivo es poder aplicarse en las elecciones al Parlamento Europeo[11].

La propuesta de este Reglamento se inserta en el marco del Plan de Acción para la Democracia europea, que adoptó la Comisión Europea en diciembre de 2020 y, concretamente, en el paquete legislativo aprobado por la Comisión el 25 de noviembre de 2021 dirigido a "Reforzar la democracia y la integridad de las elecciones"[12]. En él se incluye, amén de la PRTSP, la revisión del Reglamento sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones políticas europeas; la refundición de dos Directivas sobre el derecho de voto de los «ciudadanos móviles de la UE» (ciudadanos de la UE que residen en un Estado miembro del que no son nacionales); y una propuesta de mecanismo conjunto en materia de resiliencia electoral.

La PRTSP constituye la avanzadilla para que todos los Estados miembros aprueben normas que afectan a la materia. Llegamos mal y tarde a una exigencia jurídica —y política— ineludible: garantizar la integridad de las elecciones y los principios sobre los que se sustentan. En un mundo en línea preceptivamente y de forma análoga se tienen que aplicar escrupulosamente los principios de neutralidad e igualdad de armas que garantizan que los candidatos que concurren a las elecciones compiten en igualdad de condiciones[13].

Tras un análisis de la propuesta de Reglamento[14] y de los diversos desafíos que plantea me centraré en los efectos más inmediatos que los grandes ejes normativos sobre los que se articula la propuesta tendrán en el ordenamiento "electoral" español.

[11] COM/2021/731 final, 25.11.2021.

[12] *Vid.* La Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Proteger la integridad de las elecciones y promover la participación democrática, COM (2021) 730 final.

[13] Lo he venido denunciando hace ya varios años en diversos trabajos. Si bien, a juicio del Consejo de Europa, la falta de marco legal y el nivel insuficiente de transparencia de las campañas en línea se viene observando en la última década en relación con los intermediarios, las campañas, las técnicas los actores involucrados y el gasto electoral (Recomendación CM/Rec (2022)12 del Comité de Ministros a los Estados miembros sobre comunicación electoral y cobertura mediática de las campañas electorales, adoptado el 6 de abril de 2022).

[14] Remitimos a los interesantes dictámenes emitidos sobre el mismo por el Comité Económico y Social Europeo (CESE) [COM (2021) 731 final — 2021/0381 (COD)]; por el Comité Europeo de las Regiones (CDR) (2022/C 301/13) en el que se detallan las enmiendas que se recomiendan al Texto de la Propuesta de Reglamento de la Comisión Europea y el del Supervisor Europeo de Protección de Datos (2022/C 145/11).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.307

Obsérvese que, tal y como determina el artículo 1.1. de la PRTSP, este Reglamento establece:

> "a) obligaciones armonizadas de transparencia por las que los proveedores de publicidad política y servicios conexos deben conservar, divulgar y publicar información relacionada con la prestación de dichos servicios;
>
> b) normas armonizadas sobre el uso de técnicas de segmentación y amplificación en el contexto de la publicación, difusión o promoción de publicidad política que implique el uso de datos personales".

Se aplica "a la publicidad política preparada, insertada, promocionada, publicada o difundida en la Unión, o dirigida a personas físicas en uno o varios Estados miembros, con independencia del lugar de establecimiento del proveedor de servicios publicitarios y de los medios utilizados" (art. 1.2 PRTSP).

Los objetivos del Reglamento se cifran, según dicción literal del art. 1.3 PRTS, en:

a) contribuir al buen funcionamiento del mercado interior de los servicios de publicidad política y los servicios conexos;

b) proteger a las personas físicas en lo que respecta al tratamiento de datos personales.

Finalmente, quisiera advertir que este trabajo no abordará el uso de las TIC en las distintas fases del proceso electoral por parte de las autoridades electorales (registro en el censo electoral, firmas electrónicas para la presentación de candidaturas, transmisión electrónica de diversos datos electorales entre quienes integran la administración electoral o la publicación en línea de la información relacionada con las elecciones)[15]. Aspectos que, por cierto, también resultarían susceptibles de ser analizados desde la perspectiva de la gestión de riesgos para la integridad del proceso electoral. Sin embargo, ello excedería con mucho la extensión de este trabajo.

2.- La integridad de las elecciones en el entorno digital: una visión holística del binomio protección de datos y exigencia de transparencia en la publicidad política

Cualquier análisis riguroso que pretenda abordar las distintas amenazas que se ciernen sobre la integridad del proceso electoral no puede soslayar que el

[15] Sobre el particular remitimos a las Directrices del Comité de ministros sobre el uso de las tecnologías de la información y comunicación (TIC) en los procesos electorales en los Estados miembros del Consejo de Europa (1424ª sesión, 9 de febrero de 2022), CM (2022) 10-final.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

Reglamento General de Protección de Datos (RGPD) se aplica a todos los actores que intervienen en el contexto de unas elecciones —si bien, con matizaciones, tal y como establece el propio RGPD[16] y el margen de actuación que han implementado a tales efectos los Estados miembros en sus respectivas normativas[17]—, esto es: partidos, candidatos, autoridades públicas que organizan y controlan el proceso, intermediarios y empresas que analizan datos, plataformas de redes sociales y de publicidad en línea, etc.

El tratamiento de datos personales en el contexto de unas elecciones está sujeto a los mandatos del RGPD y a todas y a cada una de las previsiones y limitaciones que el mismo establece (consentimiento explícito, tratamiento de datos para cumplir una obligación legal o de interés público, etc.) incluidas las obligaciones de los responsables del tratamiento de datos.

Éstos, según establece el RGPD, están obligados a informar a las personas sobre el tratamiento de sus datos y muy especialmente sobre la identidad del responsable, los fines del tratamiento, fuentes de los datos, destinatarios, etc. Obsérvese que en el contexto de unas elecciones la serie de datos recogidos y tratados pertenecen muchos de ellos a la categoría de sensibles, por lo que tanto los encargados como los responsables del tratamiento tienen que aplicar medidas adecuadas para garantizar el nivel de seguridad que se exige en proporción con los riesgos que entrañan.

Apenas hace una década la doctrina iniciaba el análisis de las consecuencias y efectos en los derechos fundamentales que se vinculaban en el derecho electoral al uso indebido que de los datos de los electores realizaban los partidos políticos y los candidatos para captar el sufragio del elector durante la campaña electoral. En la actualidad el avance tecnológico hace que los objetivos y riesgos durante las elecciones sean absolutamente expansivos (en cuanto a los actores implicados) y perniciosos para el conjunto del sistema al introducirse diversas motivaciones

[16] De forma sinóptica recuérdese que el Considerando 56 del RGPD aclara el artículo 9, apartado 2, letra g): «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».

[17] Dada la extensión del trabajo, recordemos someramente que la LOREG en su el art. 58. bis. Utilización de medios tecnológicos y datos personales en las actividades electorales, es justamente expresión del margen de acción del Estado frente a lo que dispone el RGPD. Sobre la significación y efectos de la STC 76/2019, de 22 de mayo, por la que se declara la inconstitucionalidad del apartado 1 del art. 58. bis de la LOREG, véase, Arenas Ramiro, M., (2019: 342-372) y Jove Villares, D., (2021: 303-331).

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

(ideológicas, geopolíticas o simplemente cibercriminales) y variables que pueden llegar a afectar, incluso, a la propia seguridad nacional[18].

Como hemos dicho anteriormente, el uso masivo y tratamiento ilegítimo de los datos personales pueden constituir en sí un ataque a la esencia misma del sistema democrático y al funcionamiento de sus instituciones cuando se aplican técnicas de Inteligencia Artificial para la selección de usuarios y dirección de mensajes políticos.

Sobradamente conocido es que detrás de la Inteligencia Artificial se hallan los algoritmos y que éstos con el tiempo desarrollan sesgos de muy diferentes tipos que pueden conducir a la discriminación[19]. No digamos cuando se utiliza en un proceso electoral y las causas de la discriminación algorítmica se vincula directamente al núcleo duro de la ideología, sexo, opiniones políticas o creencias religiosas.

El uso de la inteligencia artificial[20], con sus algoritmos, y las aplicaciones de microsegmentación en el entorno en línea pueden servir para manipular masivamente al electorado, ya sea a través de la desinformación masiva de los ciudadanos con efecto caja de resonancia, ya sea a través directamente de *fake news*, o de perfilados que permiten dirigir información falsa a un individuo o grupos de individuos de características comunes.

En definitiva, las técnicas, instrumentos tecnológicos y las diversas aplicaciones que utilizan y se nutren de un tratamiento ilegítimo y masivo de datos personales en el contexto online y de redes sociales se convierten en el perfecto caballo de Troya para dinamitar las reglas y principios jurídicos que garantizan unas elecciones libres. Y, entre otras muchas consecuencias, contribuyen de forma decisiva a minar la

[18] Cabe recordar aquí que el Parlamento Europeo pide abordar la protección de todo el proceso electoral como "una cuestión prioritaria de seguridad nacional y de la Unión" frente a injerencias extranjeras durante los procesos electorales. De hecho, solicita a la Comisión que desarrolle un mejorado marco de respuestas para contrarrestar tales injerencias. Véase la Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2020/2268(INI)) (2022/C 347/07)) Especialmente remitimos a los puntos 83 a 93.

[19] Remitimos a los estudios de caso para probar el posible sesgo en los algoritmos publicados en el Informe de la FRA *Bias in algorithms. Artificial Intelligence and discrimination*, *op. cit.*: 25-76.

[20] Los algoritmos están insertados no solo en procesos de decisión en la Administración pública, también lo están en los productos y en los servicios que ofrece el sector privado y afectan a todos los órdenes de la realidad social y, en consecuencia, a los derechos y a las libertades.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.307

confianza de los ciudadanos sobre el cumplimiento escrupuloso de las reglas que garantizan la legitimidad del sistema[21].

Y, además, desde complejas y múltiples perspectivas, incluyen las expansivas y cada vez más sofisticadas ciberamenazas. La evaluación del riesgo sectorial cuando se ven comprometidos sectores críticos o altamente críticos como el de la infraestructura digital o proveedores de servicios digitales (que abarca entidades como proveedores de mercados en línea, de motores de búsqueda en línea o de plataformas de servicios de redes sociales)[22] resultan, más que una exigencia, una obligación por la que necesariamente deben velar los poderes públicos. No en vano, la Comisión subrayaba en su comunicación de 2018 sobre garantizar unas elecciones europeas libres y justas[23] que los ataques contra las infraestructuras electorales y los sistemas de información para las campañas electorales constituían amenazas híbridas que la Unión debía afrontar. Lo que implicaba adquirir un mayor conocimiento de las amenazas y una mayor transparencia del proceso político.

Es bien conocido que el asunto de *Cambridge Analytica* supuso un punto de inflexión en la preocupación por la influencia en la opinión pública de los votantes. Sobre lo sucedido la UE tomó buena nota y el tratamiento de los datos en el contexto de unas elecciones encontraron expresa mención en el RGPD[24] y el requisito de "transparencia" adquirió clara entidad, tal y como expresamente puso en valor la Comisión.

En efecto, "la información incompleta sobre los fines para los que se recababan los datos fue una deficiencia clave en el caso Cambridge Analytica, que también ponían en cuestión la validez del consentimiento de las personas afectadas"[25]. Y es que, ciertamente, las organizaciones que tratan datos personales en el contexto electoral tienen que asegurarse de que las personas entienden plenamente cómo se utilizarán sus datos personales y con qué fines se utilizarán antes de dar su consentimiento o antes de que el responsable del tratamiento empiece a tratarlos sobre la base de cualquier otro fundamento. Esta obligación cobra especial

[21] García Mahamut, R., (2015 a): 482).

[22] Vid. Anexo I y II de la Directiva (UE)2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022.

[23] «Garantizar unas elecciones europeas libres y justas». Contribución de la Comisión Europea a la reunión de dirigentes en Salzburgo los días 19 y 20 de septiembre de 2018, COM(2018) 637.

[24] Véase la Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre el uso de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de datos (2018/2855(RSP)).

[25] Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral COM (2018) 638 final, p.8.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

relevancia cuando son los partidos políticos los que tratan datos obtenidos de terceros. En estos supuestos tienen que informar y explicar a las personas afectadas cómo combinan y utilizan esos datos para garantizar el tratamiento leal de los mismos.

En este contexto, cómo decíamos en páginas anteriores, los datos personales de los electores constituyen el arma más poderosa sobre los que obtener una información que se perfila, se personaliza y se utiliza *por* y *a través* de las redes sociales para orquestar a gran escala campañas políticas de desinformación, manipulación y engaño[26].

Nadie puede ya soslayar el hecho de que millones de personas utilizan los medios en línea como principal fuente de información[27]. No olvidemos, como también pone de relieve Pauner Chulvi, que los propios medios de comunicación han transformado sus tradicionales formatos para incorporarlos a las redes sociales. En efecto, los periodistas ya no solo comparten noticias y opiniones en las plataformas, son los propios periódicos los que han adoptado las redes sociales como medio de distribución de noticias de última hora con absoluta inmediatez "e, incluso, los profesionales acuden a estas redes para nutrirse de historias y como fuente de información"[28].

Los proveedores de medios sociales constituyen un elemento esencial en la problemática que abordamos porque, como bien se define en las Directrices 8/2020 del Comité Europeo de Protección de Datos (CEPD), son los que ofrecen un servicio en línea que permite el desarrollo de redes de comunidades de usuarios que comparten información y contenidos. Estos servicios se ofrecen a través de navegadores web o aplicaciones. Y, en efecto, para poder prestar el servicio el proveedor determina qué datos se tratan, con qué finalidad, condiciones y forma en que se tratan los datos personales. Ello les permite obtener no solamente una cantidad ingente de datos basados en el comportamiento de sus usuarios, también el de otras personas que no están registradas. Se recopilan y combinan datos, y en consecuencia se obtiene una exponencial información, sobre actividades que se realizan tanto en la propia plataforma como fuera de ella.

[26] Dada la imposibilidad de extendernos sobre los distintos ámbitos que abarcan la desinformación en el contexto electoral remitimos a Garriga Domínguez, A. (2020: 251-287).

[27] Véase el informe del 2022 del Digital News Report, Reuters Institute, al que puede accederse a través del enlace https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2022/dnr-resumen-ejecutivo.

[28] Pauner Chulvi, C., (2022: 46).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

Los mecanismos y estrategias de focalización[29] se utilizan para influir en el comportamiento y elección de las personas socavando su libertad o autonomía personal, por ejemplo, como nos recuerda el CEPD, mediante mensajes individualizados diseñados para explotar o acentuar vulnerabilidades o preocupaciones personales. En efecto, "un análisis de los contenidos compartidos a través de los medios sociales puede revelar información sobre el estado emocional (por ejemplo, mediante un análisis del uso de determinadas palabras claves). Esta información podría utilizarse para dirigir a la persona mensajes específicos y en momentos concretos en los que se espera que sea más receptiva e influir así subrepticiamente en su proceso de pensamiento, sus emociones y su comportamiento"[30].

Es un hecho objetivo que la publicidad política juega un papel absolutamente relevante en la formación de la opinión de los ciudadanos durante todo el proceso electoral y especialmente durante la campaña electoral. La publicidad política, tal y como se define por la Comisión en la propuesta de Reglamento, significa "la preparación, colocación, promoción, publicación o difusión por cualquier medio de un mensaje: por, para o en nombre de un actor político, a menos que sea de naturaleza puramente privada o comercial; o que pueda influir en el resultado de una elección o referéndum, un proceso legislativo o reglamentario o el comportamiento electoral".

La publicidad política patrocinada está planteando en los entornos en línea problemas de enorme envergadura al entramado de garantías jurídicas sobre las que se sustentan los procesos electorales en los sistemas democráticos.

No debe perderse en modo alguno de vista que las tecnologías digitales y las redes sociales constituyen el caldo de cultivo definitivo para una publicidad política que con apariencia de ofrecer información neutra lo que directamente persigue es la difusión de información falsa, a través de distintos mecanismos que permiten difundir y repetir una y otra vez una idea o información falsa con el objeto claro de manipular a los votantes con el terrible efecto no solamente de conculcar los derechos más básicos sobre los que descansan las reglas de la competición electoral. A más, lo que puede hallarse realmente en juego es la pervivencia del sistema democrático de un país objeto de ataque de una potencia extranjera cuyo objetivo puede no ser otro que generar inestabilidad política cuando no el cambio

[29] Sobre el particular, véase las Directrices 8/2020 sobre la focalización de los usuarios de medios sociales del Comité Europeo de Protección de datos, de 13 de abril de 2021. Obsérvese que la focalización, siguiendo la estructura de estas directrices, puede basarse en datos facilitados por el usuario —al proveedor de medios sociales y en los facilitados por el usuario de la plataforma de medios al focalizador—; en datos observados y en datos inferidos.

[30] *Ibidem*, p.7.

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

de un gobierno por otro por motivos bien variados (geopolíticas, cibercriminales, etc.).

Téngase presente que los motores de búsqueda y las plataformas de redes sociales estructuran y organizan la información. Mediante los algoritmos y a través de procesos automatizados las plataformas seleccionan y priorizan noticias afectando a la libertad de información, aunque también es cierto que a través de la implementación de los algoritmos las plataformas pueden bloquear contenidos, discursos, etc., para luchar contra comportamientos ilegales, cuando no delictivos.

En todo este oscuro y resbaladizo escenario son diversas y complejas las ramificaciones de una problemática jurídica que horada la confianza ciudadana en los medios y en las soluciones. No es de extrañar porque en algunos Estados miembros la publicidad política en línea no está sujeta a las normas que se aplican fuera de línea. De hecho, en ocasiones, ni los reguladores están en disposición de cumplir con la obligación de vigilar el límite de gastos en este tipo de publicidad y evitar así fuentes ilegales de financiación con las consecuencias que ello acarrea para la propia integridad del proceso electoral.

No puedo estar más de acuerdo con la afirmación de que la falta de transparencia en la financiación no solo amplía los márgenes para la corrupción, sino que invita a inversiones extranjeras de dudosa legalidad en sus pretensiones. La exigencia de una serie de requisitos sobre la transparencia de esa publicidad es el principio primario sobre el que actuar, pero no el único. El uso indebido de datos personales confidenciales por parte de las plataformas y servicios digitales, así como su utilización para la microsegmentación, constituyen una gravísima amenaza para el interés público.

Saber quién está detrás y quién financia la publicidad con fines electorales constituye una exigencia jurídica ineludible en cualquier sistema democrático. Por ello, tanto la práctica de este tipo de publicidad —que no solo puede resultar abusiva sino decididamente manipulativa y en sí misma transfronteriza— debe estar claramente definida, supervisada y controlada en todos sus frentes[31]. Dos son los grandes retos en este ámbito: dotar de un elevado y riguroso nivel de transparencia a la publicidad política y a sus proveedores de servicios y responsables de los tratamientos de datos y a la protección de los datos personales del y en el entorno digital.

[31] De ahí la importancia de exigir, para garantizar la transparencia, la identidad del patrocinador del anuncio político, así como la de la entidad que controle en última instancia al patrocinador. En esta línea también se muestra unánime el Consejo de Europa en su comunicado sobre Transparencia y segmentación de la publicidad política de 13 de diciembre de 2022.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

La manipulación en línea toma como elemento esencial el uso ilegítimo de los datos personales. Esa ha constituido la principal razón para que la Comisión presentara la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la transparencia y la segmentación política el 25 de noviembre de 2021, precisamente, para garantizar elecciones y referendos más transparentes y resistentes con el fin de poderse aplicar a las elecciones al Parlamento Europeo en el 2024.

3.- La propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la transparencia y la segmentación de la publicidad política: Principales objetivos

En la UE no hay un marco jurídico común que regule el uso de la publicidad política que realizan los partidos políticos europeos cuando concurren a las elecciones europeas. Ciertamente, los Estados miembros tienen su propia normativa sobre publicidad política. Sin embargo, a juicio de la Comisión, esta legislación cuando afecta directamente a los proveedores de servicios puede, por la diversidad regulatoria que se da en cada Estado miembro, generar obstáculos a la publicidad política como servicio transfronterizo en el mercado interior[32]. Una de las razones, por cierto, por las que también se impulsa la propuesta de Reglamento y por la que se designa comisión líder en el Parlamento Europeo a la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo (IMCO). No obstante, resulta absolutamente desconcertante que no se le haya atribuido la competencia a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE) que debería ser la comisión competente para el fondo —aunque finalmente participara como asociada de conformidad con el art. 57 del Reglamento de Procedimientos— por afectar a derechos fundamentales, entre ellos, al derecho a la protección de datos, uno de los pilares esenciales sobre los que descansa y afecta la propuesta de Reglamento.

Los datos personales se utilizan, en efecto, "para segmentar los mensajes políticos enviados a los ciudadanos dirigiendo los anuncios a grupos y adoptando el contenido"[33]. Las técnicas de segmentación en los anuncios políticos llevan aparejadas la exponencial capacidad de manipulación al poderse focalizar en grupos tan pequeños que permite incluso de forma nada transparente transmitir mensajes políticos personalizados. Ello tiene claras consecuencia en el proceso

[32] No deja de llamar suficientemente la atención la vertiente absolutamente economicista que se trata de conjugar junto con la salvaguarda de derechos fundamentales en un contexto tan relevante como unas elecciones.

[33] Documento de trabajo de los servicios de la Comisión. Resumen de la evaluación de impacto que acompaña al documento Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la transparencia y la segmentación de la publicidad política, SWD/2021/356 final.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

democrático porque la manipulación cobra vida propia y absolutamente independiente.

De ahí que en esta doble combinación los objetivos generales que persigue la Propuesta de Reglamento sean: "1) facilitar la prestación de publicidad política y servicios conexos en el mercado interior, contribuyendo al mismo tiempo a procesos democráticos justos basados en normas de transparencia elevadas y armonizadas y el uso lícito de técnicas de segmentación; 2) establecer normas de transparencia estrictas para los partidos políticos de la UE en apoyo de unas elecciones libres y justas."[34].

Por su parte, y a pesar de su extensión, conviene reproducir textualmente los objetivos específicos que se cifran en : "a) reducir la fragmentación jurídica, eliminar obstáculos y reducir los costes de los servicios transfronterizos, b) definir requisitos de transparencia elevados para los anuncios políticos (incluidos los anuncios temáticos), c) abordar los riesgos específicos de protección de datos derivados del uso de algunas técnicas de segmentación y amplificación, d) garantizar una supervisión eficaz de las obligaciones previstas y reforzar los resultados normativos, e) promover una mayor transparencia y unas elecciones libres y justas mediante el cumplimiento de las normas por parte de los partidos políticos en la UE."

No puedo menos que compartir que, en efecto, se debe aportar mayor transparencia a la segmentación y aumentar significativamente la exigencia de los requisitos de transparencia en los procesos democráticos a la vez que se debe proteger de la manipulación dando luz y taquígrafo a las técnicas de segmentación. Obsérvese que las técnicas de segmentación se utilizan para dirigir un anuncio político de forma absolutamente personalizada a una única persona o grupo específico de personas. En este punto conviene recordar que el Supervisor Europeo de Protección de Datos (SEPD) en su Dictamen 3/2018, sobre la manipulación en línea y los datos personales, y en el Dictamen 1/2021, sobre la propuesta de Reglamento de Servicios Digitales, manifestaba su honda preocupación por los riesgos relacionados con la publicidad segmentada. De modo que, frente a la propuesta de Reglamento adoptada por la Comisión Europea, el SEPD consideró que la misma debía ir más allá estableciéndose restricciones adicionales al tratamiento de los datos personales en la segmentación de este tipo de publicidad. Por ello instó a los colegisladores a incorporar normas más estrictas "(1) estableciendo una prohibición total de la microsegmentación con fines políticos; y (2) introduciendo nuevas restricciones a las categorías de datos que pueden tratarse con fines de publicidad política, incluida la

[34] Ibidem.

CC BY SA

DOI: https://doi.org/10.51915/ret.307

segmentación y la amplificación, en particular prohibiendo la publicidad segmentada basada en el seguimiento generalizado"[35].

El otro pivote sobre el que bascula, aunque de manera más indirecta, una de las finalidades que persigue la propuesta de Reglamento es evitar que otros agentes puedan influir en el resultado de una elección, referéndum, proceso legislativo, o reglamentario o un comportamiento electoral a través de la promoción, publicación, entrega o difusión de mensajes.

Aquí cobran especial relevancia las contribuciones económicas de partidos u organizaciones cuya sede se halle fuera de la UE. A estos efectos resulta de gran interés la Sentencia del Tribunal General de 25 de noviembre de 2020 en el asunto T-107/19 en la que se afirma que un partido de un país que no pertenece a la UE no entra en la definición de "partido político" al no tratarse de ciudadanos de la UE ni estar reconocido por el ordenamiento jurídico de al menos de un Estado miembro, o establecido de conformidad con este. En consecuencia, el Tribunal considera que las contribuciones de los partidos miembros con sede en países no pertenecientes a la UE pueden seguir interpretándose como prohibidas[36].

4.- Una visión de conjunto de las enmiendas aprobadas por el Parlamento Europeo: La apuesta por garantizar la transparencia y la protección de datos

El 2 de febrero de 2023 el Parlamento Europeo aprobó, en primera lectura, las enmiendas (274) a la propuesta de Reglamento[37]. Desde una perspectiva metodológica quisiera advertir que me referiré a la propuesta originaria de la Comisión o al texto que ya incluye las enmiendas aprobadas por el Parlamento Europeo, en cuyo caso, quedará advertido.

Armonizar la normativa que incide en las elecciones sobre la publicidad política ha exigido al legislador comunitario definir qué debe y qué no debe entenderse como tal. La diversidad en las legislaciones nacionales complica sobremanera la posibilidad de ofrecer un modelo homogéneo de definición.

Como se reconoce en el Considerando 15, no existe una definición de publicidad política o de anuncio político a escala de la UE. Siendo consciente de la necesidad de aportar una definición común para poder aplicar obligaciones armonizadas de transparencia, normas sobre segmentación y entrega de anuncios, la definición necesariamente tiene que abarcar las diversas normas que puede adoptar la

[35] Diario Oficial de la Unión Europea, 1/4/2022, (2022/C 145/11).

[36] Véase sobre el particular el Dictamen del Tribunal de Cuentas Europeo 01/2022 sobre la propuesta de la Comisión de Reglamento sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones políticas europeas.

[37] COM (2021)0731 – C9-0433/2021 – 2021/0381 (COD).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.307

publicidad política "y cualquier medio y modo de publicación o difusión dentro de la Unión, con independencia de que la fuente esté situada en la Unión o en un tercer país"[38].

Partiendo de esta premisa merece la pena reproducir textualmente la enmienda al Considerando 16, aprobada en primera lectura por el PE, que amplía la definición y concepto de publicidad política:

> "La definición de publicidad política debe incluir la publicidad *preparada, insertada, promocionada*, publicada, *entregada* o difundida directa o indirectamente por un actor político *o preparada, insertada, promocionada, publicada, entregada o difundida, por cualquier medio, directa o indirectamente en nombre de un actor político* o por su cuenta. Dado que los anuncios realizados por un actor político, en su nombre o por su cuenta no pueden separarse de su actividad en cuanto actor político, cabe presumir que pueden influir en el debate político *o en el resultado de una elección o referéndum*, salvo en el caso de mensajes de carácter estrictamente privado o estrictamente comercial.
>
> *A fin de determinar si el carácter de un mensaje es estrictamente privado o estrictamente comercial, deben tenerse en cuenta todos los factores pertinentes tales como: su contenido, el lenguaje utilizado para transmitirlo, el contexto en el que se transmite, su objetivo y los medios por los que se promociona, publica o difunde. Los mensajes relativos a la situación familiar o las actividades empresariales de un actor político pueden ser estrictamente privados o estrictamente comerciales. Además, la definición de publicidad política debe incluir mensajes preparados, insertados, promocionados, publicados, entregados o difundidos que puedan influir en el resultado de una elección o referéndum, en un proceso legislativo o reglamentario o en el comportamiento electoral. Estos mensajes no pueden considerarse puramente privados o comerciales. Estos mensajes pueden proceder de cualquier persona física o jurídica, incluso de fuentes oficiales, como Gobiernos, autoridades públicas, instituciones u organismos. No obstante, si sus mensajes se limitan estrictamente al anuncio de elecciones o referendos o a las modalidades de participación en elecciones o referendos, quedarán excluidos del ámbito de aplicación*"[39].

Debe destacarse que la definición de publicidad política propuesta en la enmienda no solo incluye mensajes preparados, insertados, promocionados, publicados o difundidos que puedan influir en el resultado de una elección o referéndum, también

[38] Considerando 15.

[39] Enmienda 18, Considerando 16. El texto en cursiva es el que adiciona el PE.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

añade las que puedan influir en un proceso legislativo o reglamentario o en el comportamiento electoral.

Obsérvese que el Considerando 17 de la propuesta de la Comisión señala expresamente que debe constituir publicidad política la publicación o difusión "por parte de otros agentes" de un mensaje que pueda influir en el resultado de una elección, referéndum… o un comportamiento electoral. Por el contrario, según el tenor del Considerando 19, no deben estar incluidas en el ámbito de aplicación del Reglamento las opiniones políticas que se expresan en los programas de radiodifusión audiovisual lineal o publicadas en medios de comunicación impresos sin pagos directos o remuneración equivalente. En cambio, "no debe constituir publicidad política" a juicio del Parlamento, y así lo ha reflejado expresamente:

- La comunicación de un partido político a sus miembros actuales o *antiguos* dado que ello es parte inherente la pertenencia a un partido. A mi juicio, el empleo del término antiguo no habilita en modo alguno el tratamiento de los datos personales de quienes se dan de baja en un partido político.

- La información práctica que procede de las fuentes oficiales y estrictamente limitada al anuncio de elecciones o referendos o sobre las modalidades de participación en los mismos. Es decir, lo que en la LOREG se recoge como campañas institucionales.

- Los mensajes estrictamente privados o estrictamente comerciales, aunque sean de los actores políticos o del gobierno. Para determinarlo[40] se deberá tener en cuenta contenido, lenguaje utilizado, contexto en el que se transmite, objetivo, medios por los que se transmiten, los relativos a la situación familiar o a la actividad comercial.

- Los mensajes compartidos por los particulares a título meramente personal. Ahora bien, no puede considerarse que las personas actúan a título personal si publican mensajes cuya difusión o publicación conlleva una remuneración o prestaciones en especie por parte de terceros.

Por lo que afecta a las normas sobre transparencia establecidas en el Reglamento:

-Solo deben aplicarse a la publicidad política que se presta a cambio de una remuneración o de una prestación en especie (Considerando 29). Sin embargo, no deben aplicarse al intercambio de información a través de servicios de comunicación electrónicas (servicios de mensajería electrónica o llamadas telefónicas) siempre y cuando no intervenga ningún servicio de publicidad política (Considerando 30).

[40] Adición al Considerando 16 a través de la enmienda 18.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

-Para garantizar la eficacia de los requisitos de transparencia los proveedores de servicio de publicidad política deben velar "porque la información pertinente que recojan en la prestación de sus servicios, incluida la indicación de que un anuncio es político, se proporcione al editor de publicidad política que lleve la publicidad política al público" para lo que los proveedores deberán favorecer la posibilidad de automatizar la transmisión de información entre los proveedores de servicios de publicidad política (Considerando 34).

-Las obligaciones de transparencias deben aplicarse a la entidad que preste esencialmente el servicio publicitario, así se evita eludir la eficacia de las obligaciones de la transparencia a estructuras comerciales artificiales. No obstante, como establece el Considerando 37, "ninguna de las obligaciones establecidas en el presente Reglamento debe entenderse en el sentido de que impone a los proveedores de servicios intermediarios una obligación general de supervisión de los contenidos políticos compartidos por personas físicas o jurídicas, ni debe entenderse que impone una obligación general a los proveedores de servicios intermediarios de adoptar medidas proactivas en relación con contenidos o actividades ilícitos que dichos proveedores transmiten o almacenan".

Los servicios de publicidad política se deben prestar de forma transparente de conformidad con las obligaciones que establecen los artículos 5 a 11 y 14 de la PRTSP. En una visión de conjunto el art. 5 versa sobre la identificación de los servicios de publicidad política; el art. 6 sobre el mantenimiento de registros y transmisión de información. Los requisitos de transparencia de "cada anuncio político" se regula en al art. 7. El art. 8 obliga a los editores de publicidad a incluir los estados financieros anuales la información sobre los importes por dichos servicios, "incluido el uso de técnicas de segmentación y amplificación, agregados por campaña, como parte de su informe de gestión…". El art. 9 establece los mecanismos de denuncia por parte de los particulares a los editores de publicidad de los anuncios políticos que no cumplen lo dispuesto en el Reglamento. Por su parte, el art. 10 versa sobre las facultades de las autoridades nacionales para solicitar de los proveedores de servicios de publicidad política la información a la que aluden los artículos 6, 7 y 8 y el art. 11 hace referencia a la transmisión de información a otras autoridades interesadas.

En esta línea, y en íntima conexión con las enmiendas presentadas al Proyecto por el Parlamento Europeo[41], debe destacarse que "solo los datos personales facilitados de manera explícita para la publicidad política pueden ser utilizados por los

[41] Se han presentado 274 enmiendas. Véase el Proyecto de resolución legislativa del Parlamento Europeo.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

anunciantes"[42]. En la práctica ello supondría prohibir la microsegmentación[43]. En efecto, se propone restringir las estrategias de segmentación y prohibir totalmente el uso de datos de los menores de edad.

Al objeto de evitar las interferencias extranjeras, el PE propone prohibir financiar la publicidad política dentro de la UE a las organizaciones no domiciliadas en la UE. Se han presentado enmiendas que redundan en garantizar una mayor transparencia, por ejemplo, proponiendo que los ciudadanos, periodistas y autoridades puedan acceder de forma sencilla a la información sobre publicidad política. De hecho, se plantea crear una base de datos digital para todos los anuncios políticos en línea y datos relacionados. Como se precisa en la nota de prensa del PE: "El objetivo es facilitar la obtención de información sobre quién paga los anuncios, su coste y el origen del dinero utilizado". Y en este aspecto lo más relevante es la obligación de que se convierta en información pública el que un anuncio haya sido suspendido por violación de las reglas, los grupos específicos de individuos a los que van dirigidos, y los datos personales utilizados, las visitas y las acciones de la audiencia respecto del anuncio para así garantizar de forma específica el derecho de los periodistas a obtener esa información.

Otro de los elementos que más fricción genera a la hora de establecer ciertos límites son los que se vinculan a la libertad de editorial de los medios de comunicación. Partiendo de la premisa de que el futuro Reglamento de publicidad política no debe afectar a la libertad de editorial de los medios de comunicación, se argumenta que "Los puntos de vista políticos y las opiniones u otros contenidos editoriales expresados o difundidos con fines periodísticos o bajo la responsabilidad editorial de un proveedor de servicios de comunicación no deben considerarse publicidad política y no deben estar incluidos en el ámbito de aplicación del presente Reglamento, si no hay terceros que proporcionen un pago u otra remuneración específicamente por la expresión de los puntos de vista u opiniones. Las percepciones y opiniones políticas de este tipo que, además, sean promocionadas, publicadas o difundidas por el proveedor de servicios deben considerarse en todos los casos publicidad política. Deben aplicarse las prácticas periodísticas establecidas en la legislación nacional o por los consejos de medios de comunicación o de prensa de conformidad con el Derecho de la Unión, incluida la Carta de los Derechos Fundamentales (CDF). Se debe prohibir cualquier forma de publicidad encubierta."[44].

[42]Tal y como textualmente se explicita en la Nota de prensa del PE, de 2 de febrero de 2022, bajo el título "El Parlamento quiere reglas más estrictas para la publicidad política".

[43] La microsegmentación es una estrategia que utiliza los datos de consumo y demográfico para identificar los intereses de individuos específicos.

[44] Enmienda 24, Propuesta de Reglamento, Considerando 19.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

No obstante, sí que se adiciona en el Considerando 24 la excepción de que no haya terceros que proporcionen un pago o remuneración específica por la expresión o de los puntos de vista u opiniones. En efecto, "Las percepciones y opiniones políticas de este tipo que, además, sean promocionadas, publicadas o difundidas por el proveedor de servicios deben considerarse en todos los casos publicidad política".

Se prevé la aplicación del Reglamento a la publicidad comercial cuando ésta pueda ser la responsable de influir en el resultado de una elección o referéndum, proceso legislativo o reglamentario, o en un comportamiento electoral. La propuesta de Reglamento expresamente establece que el mismo complementa al ya hoy vigente Reglamento de Servicios Digitales (RSD). Así, mientras que el RSD impone requisitos de transparencia a las plataformas en línea "esta iniciativa abarca todo el espectro de editores de publicidad política, así como otros proveedores de servicios pertinentes que intervienen en la preparación, inserción, promoción, publicación y difusión de publicidad política".

En relación con ello, y por lo que afecta a los intermediarios en línea, el RSD se aplica a los anuncios políticos publicado o difundidos por intermediarios en línea a través de normas horizontales aplicables a todos los tipos de publicidad en línea, incluidos los anuncios comerciales y políticos.

Pues bien, partiendo de la definición de publicidad política el Parlamento estima conveniente, y de ahí la enmienda 43 presentada al Considerando 32, proporcionar un mayor grado de detalle a los requisitos de transparencia fijados para los editores de publicidad que entran en el ámbito de aplicación del ya hoy aprobado RSD, Y si bien, como proponía la Comisión en su propuesta de Reglamento, los requisitos no afectan a las disposiciones del RSD, a juicio del Parlamento "deben servir de base de cara a las obligaciones de evaluación y mitigación de riesgos para las plataformas en línea de muy gran tamaño en relación con sus sistemas de publicidad, *incluidas las técnicas de segmentación y entrega de anuncios de los servicios de publicidad política empleados*. Con el fin de ayudar a los Estados miembros y a los proveedores de servicios, la Comisión debe proporcionar directrices sobre la interacción entre los distintos actos jurídicos de la Unión y el presente Reglamento, así como su naturaleza complementaria, y sobre la interpretación de requisitos similares contenidos en ellos".

No cabe perder de vista que la propuesta de Reglamento se incluye dentro de un paquete electoral entre las que se cuenta la Recomendación sobre las redes de cooperación electoral, la transparencia en línea, la protección contra incidentes de ciberseguridad y de lucha contra las campañas de desinformación.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

5.- Una aproximación sobre los efectos del Reglamento de transparencia en el régimen electoral español

Quisiera comenzar recordando algo, por ahora, obvio: los responsables de la organización y control del proceso electoral en cada Estado miembro de la UE son los propios Estados.

Dada la limitación del trabajo, y ciñéndome a nuestro modelo de Administración electoral, no cabe duda de que la LOREG rompe absolutamente todas sus costuras cuando se trata de garantizar que en las campañas digitales se cumplan con los estrictos mandatos legales de garantía de igualdad de oportunidades entre los contendientes electorales.

Como he reiterado en diversos trabajos hace ya demasiado tiempo que la salvaguarda del principio de neutralidad y, especialmente, el de igualdad de armas entre quienes concurren a las elecciones ya no peligra en el terreno de lo presencial sino en el ciberespacio.

Nuestro legislador orgánico, hace ya tiempo que debía haber abordado en la LOREG algunas de las cuestiones más candentes que afectan, entre otros, a la transparencia de los mensajes publicitarios en las campañas electorales en red. Exigir jurídicamente mayor transparencia en "la publicidad" política de las campañas en línea y fortalecer en todos sus flancos las facultades de control y supervisión de las Juntas Electorales, especialmente de la JEC, constituyen deberes ineludibles de los poderes públicos en nuestro ordenamiento con o sin Reglamento Europeo. Sin duda, deben quedar expresamente prohibidas aquellas técnicas de segmentación que utilicen datos personales sin consentimiento expreso y aunque ello pudiera deducirse de otros preceptos del derecho europeo, constitucional y/o de legislación orgánica, lo cierto es que en aras de la seguridad jurídica debemos avanzar decididamente en este mundo en red donde la integridad del proceso electoral puede verse seriamente amenazada a la par que las reglas del juego democrático que regulan la alternancia en el poder.

En este escenario no puedo soslayar el hecho de que la Junta Electoral Central hace tiempo que afirmó que los principios del proceso se aplicaban también en las campañas en el entorno digital. Pero esto, a mi juicio, termina funcionando en cierta manera como del lado oscuro del *soft low*[45].

[45] Sobre el concepto de *soft.-law* de las certificaciones que se encuentran en el mercado, véase Viguri Cordero, J. (2021: 162).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

Las Juntas electorales no disponen de medios humanos ni económicos que permita hacer frente a una labor de enorme complejidad desde cualquier perspectiva técnica y metodológica con la que se debe hacer frente, por no mencionar la ausencia de recursos humanos altamente cualificados en el ámbito tecnológico, que permita integrar en nuestro modelo de control de las elecciones el conocimiento interdisciplinar. No hay medios, no hay recursos, y lo más grave: carecemos de una metodología para abordar una reforma de las estructuras de control y supervisión coordinadas y eficientes que permitan garantizar en esta realidad, no en la del siglo pasado, la integridad del proceso electoral.

Uno de los mayores problemas que plantea la aplicación del futuro Reglamento en el ordenamiento español es precisamente una de las consecuencias que, en mi opinión, lleva aparejada: coordinar los distintos roles que deberán desempeñar en esta materia las autoridades de control de protección de datos y la Administración Electoral que es la que tiene por finalidad "la transparencia y objetividad del proceso electoral y del principio de igualdad" (art. 8.1 LOREG)

A mi juicio, debemos definir absolutamente los procedimientos y los roles a desempeñar por las distintas autoridades y administraciones independientes. También un procedimiento sancionador que conjugue la vulneración de las reglas del juego de un proceso electoral junto con la de protección de los datos cuando este sea el elemento vehicular para socavar las reglas y principios sobre los que se basan unas elecciones libres. Ello no resulta viable si no se diseña una eficaz coordinación, no solamente comunicación, entre las autoridades de control de protección de datos y las juntas electorales, por no mencionar a las autoridades en materia de transparencia y aquellas otras que ejercerán sus funciones en el ámbito del Reglamento Europeo de Datos.

No olvidemos que las autoridades de protección de datos deben hacer cumplir la aplicación de los principios de protección de datos también durante todo el proceso electoral. Tampoco podemos perder de vista que las autoridades de protección de datos de cada Estado miembro, tal y como mandata el propio RGPD, deben garantizar la cooperación y la coherencia de sus acciones en el CEPD.

Sin embargo, la superposición de autoridades diversas en la normativa comunitaria, lejos de garantizar la seguridad jurídica exigible terminarán en mi opinión difuminando el uso efectivo de los controles. Aunque se afirme en la propuesta de Reglamento que no se prevé la creación de autoridades o u organismos adicionales en cada Estado miembro "los Estados miembros podrían designar a las autoridades sectoriales existentes a las que también confiarían las competencias para vigilar y aplicar las disposiciones del Reglamento, aprovechando así sus conocimientos especializados. Los Estados miembros serán responsables de garantizar que estas

CC BY SA

DOI: https://doi.org/10.51915/ret.307

autoridades tengan la capacidad necesaria para garantizar la protección de los derechos de los ciudadanos en el contexto de una publicidad política transparente".

Creo que ha llegado el momento en el que se debe exigir jurídicamente, probablemente mediante ley, la obligación de implementar por parte de los órganos que en nuestro país tienen que actuar en la organización, control y garantía de las de las elecciones un enfoque de gestión de riesgos en coordinación con otras autoridades (protección de datos y transparencia, entre otras). No avanzaremos lo suficiente si no se obliga a los distintos actores que organizan y controlan las elecciones, así como a los que tienen competencia en la materia en el ámbito de la seguridad nacional, a dar cuenta de todos los riesgos que se han observado y detectado en las concretas elecciones. Una vez más se impone la constitución interdisciplinar de grupos que con responsabilidad en las actuaciones públicas estudien las incidencias y prevean riesgos futuros. No podemos sin más remitirnos a normativas europeas que, como no puede ser de otro modo, dejan un amplio margen de implementación por parte de los Estados miembros.

No quisiera dejar de referirme a un elemento que cobra cada vez más una mayor fuerza y sobre la que España ha mostrado un mayor alejamiento de forma tradicional. Me estoy refiriendo a ese tipo de publicidad difamatoria y campañas injuriosas que fabrican y difunden deliberadamente información falsa sobre actores políticos con el fin de perjudicar su imagen pública. Esta es una enmienda que se ha propuesto como Considerando 4 bis nuevo y que emplaza a los Estados miembros a adoptar todas las medidas necesarias para poner fin a tales prácticas y para investigarlas especialmente durante los períodos electorales.

Obsérvese que, por otro lado, ya empezamos a contar con acciones por parte de algunas de las plataformas sociales que gestionan redes sociales, en cumplimiento de medidas autorregulatorias y de códigos de buenas prácticas, que deciden cerrar la cuenta o el perfil de candidatos en plena campaña electoral que merecen ser reflexionados y sistematizados en la normativa electoral[46]. Sin duda, deben gestionarse los mecanismos de denuncias y diseñar normativamente la articulación procedimental para solicitar alegaciones y exigir responsabilidades sobre determinadas acciones de las plataformas para quienes, frente a las denuncias, corresponde garantizar la objetividad, neutralidad y transparencia del proceso electoral que en nuestro país son las Juntas Electorales. Singularmente la acción de la Junta Electoral Central (JEC) en esta materia adquiere una especial importancia.

[46] A estos efectos resulta de gran interés el Acuerdo del JEC 146/2021, de 14 de febrero. Acuerdo que se adopta al hilo de la denuncia de VOX porque Twitter había suspendido la cuenta del cabeza de lista de la circunscripción de Barcelona. Sobre las medidas autorregulatorias y códigos de buenas prácticas (Viguri Cordero, J., 2021: 169).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.307

Garantizar la integridad de unas elecciones, y la confianza ciudadana, depende de que se garantice efectivamente el cumplimiento de un marco legislativo coherente que dote de plena seguridad jurídica la acción de todos los actores electorales. También la de los intermediarios privados –medios y plataformas digitales– y, cómo no, la de los operadores jurídicos que deben velar por la aplicación de las normas que garantizan el ejercicio efectivo de los derechos fundamentales de participación política en unas elecciones libres en las que en ningún caso se pueda utilizar sin consentimiento expreso en su vis más restrictivas, salvando las expresas excepciones normativas, el derecho a la protección de datos.

6.- Reflexiones conclusivas

Hace ya tiempo que vengo denunciando que en los procesos electorales en nuestro ordenamiento ni se ha prestado, ni se presta, la necesaria atención jurídica a las consecuencias que acarrean el uso masivo y tratamiento ilegítimo de los datos personales en un contexto de constante revolución tecnológica en un mundo en red. La atención jurídica, desde la perspectiva del cumplimiento y garantía de las reglas del juego democrático, se ha centrado fundamentalmente en el mundo presencial y en los medios difusión y comunicación tradicionales, así como si los distintos actos que realizan quienes concurren a las elecciones se financian públicamente y si se realizan en período de campaña electoral o fuera de ella.

No resulta en absoluto razonable que con el uso que realizan en unas elecciones —aunque no solo— los partidos y candidatos de las redes sociales y de las diversas plataformas digitales durante toda la campaña electoral, en la LOREG no exista ninguna disposición expresa que regule todos los aspectos que afectan a la misma del mismo modo que lo hace cuando de forma milimétrica regula la aparición de los candidatos ante los medios de comunicación social para garantizar los principios de pluralismo e igualdad y los principios de proporcionalidad y de neutralidad informativa, tanto en la programación de los medios de titularidad pública en período electoral, como en los debates y entrevistas electorales y en la información relativa a la campaña electoral para las emisoras de titularidad privada (arts. 66 y 67 de la LOREG)[47].

En el entorno virtual no es fácil para el ciudadano, y a veces tampoco para quienes concurren a las elecciones, reconocer si se está ante un anuncio político o no o ante una estrategia de desinformación masiva en cualquiera de sus múltiples facetas. No digamos para que actúe con la inmediatez que exigen los plazos electorales quienes se encargan en nuestro país de garantizar la transparencia y la objetividad del proceso electoral y del principio de igualdad del proceso electoral, tal y como he

[47] García Mahamut, R., (2015 b): 324).

CC BY SA

DOI: https://doi.org/10.51915/ret.307

venido denunciando[48]. En efecto, la JEC carece de medios para realizar un control efectivo de tos estos ámbitos en este tipo de campañas en el mundo en red. Excede con mucho de sus capacidades, organización, funcionamiento, medios materiales y recursos humanos.

En el proceso electoral transparentar a "los sujetos" que se hallan detrás de los anuncios y de la publicidad política constituye una exigencia jurídica ineludible para evaluar y ponderar con cierto éxito si la información que se recibe por este medio es objetiva y no constituye en sí misma una manipulación en sus diversas variables.

Sin duda, la UE ha dado un paso al frente de notable envergadura con la propuesta de Reglamento que contiene obligaciones armonizadas para los editores y proveedores de publicidad política e introduce normas sobre el uso de técnicas de segmentación y amplificación de la publicidad política.

Una de las cuestiones para tener en cuenta es que, como se encarga de subrayar la Comisión, el Reglamento se basa y complementa la legislación pertinente de la UE incluido el RGPD. Sin embargo, a mi juicio, este Reglamento estrecha sectorialmente su contenido material en el ámbito de la publicidad lo que reviste una complejidad tremenda y resta seguridad jurídica. En mi opinión, la evaluación de impacto relativa a la protección de datos a la que alude el RGPD cuando el tratamiento de datos entraña un alto riesgo para los derechos y libertades de las personas (art. 36 y 36 RGPD) no se ha llevado a cabo con la diligencia debida.

Por un lado, obsérvese que la enmienda 112 al art. 1, apartado 4 bis nuevo del PE precisa que: "Las normas de protección de datos relativas al tratamiento de los datos personales operativos contempladas en el presente Reglamento se considerarán normas específicas de protección de datos en relación con las normas generales que se establecen en los Reglamentos (UE) 2016/679 y (UE) 2018/1725. Ninguna de las disposiciones del presente Reglamento puede aplicarse o interpretarse de forma que disminuya o limite el nivel de protección que brindan el derecho al respeto de la vida privada y de la protección de datos y el derecho a la libertad de expresión, tal como se protegen en la CDF y en la legislación de la Unión en materia de protección de datos y privacidad, en particular en los Reglamentos (UE) 2016/679 y 2018/1725".

Por otro lado, repárese en que la supervisión del Reglamento se deberá realizar por las autoridades de supervisión y competencias para hacer cumplir las normas y "En función del ordenamiento jurídico de cada Estado miembro y de conformidad con la legislación vigente de la Unión, incluidos el Reglamento (UE) 2016/679 y el Reglamento (UE) 2022/2065 (de Servicios Digitales), podrán designarse diferentes

[48] En la misma línea Sánchez Muñoz, O., (2020: 278 y 279).

Sección Estudios y Artículos
Elecciones, protección de datos y transparencia en la publicidad política …
por Rosario García Mahamut
Págs. 75-105
DOI: https://doi.org/10.51915/ret.307

autoridades judiciales o administrativas nacionales a tal efecto"[49]. Por si ello no fuera suficiente, se prevé que para la supervisión de aquellos aspectos de este Reglamento que no sean competencia de las autoridades de control en virtud de los establecido en el RGPD, en el Reglamento 2018/725 y en el nuevo Reglamento de Servicios Digitales, los Estados miembros tienen que designar a las autoridades competentes para supervisar y hacer cumplir las normas pertinentes.

A lo anterior hay que sumar la complejidad añadida que incorporaría la aprobación de lo que actualmente prevé la propuesta de la Comisión de Reglamento sobre la financiación de los partidos políticos europeos y las fundaciones políticas europeas[50], en una lectura conjunta de lo que dispone esta propuesta de Reglamento y la PRTSP en lo que afecta a la participación de las autoridades reguladoras nacionales y su cooperación. Comparto la misma opinión que el Tribunal de Cuentas Europeo cuando afirma que "existe un riesgo de solapamiento de competencias, por ejemplo, en lo que respecta al control de las normas de publicidad política y a la transmisión de información sobre esta"[51] y sugiere que se revisen las responsabilidades de cada organismo de control en cuestión.

En esta línea, y dado que ambas propuestas de Reglamentos se tramitan en paralelo, no podemos obviar que la propuesta incorpora disposiciones relativas a la publicidad política cuyo objeto de desarrollo se halla en la PRTSP objeto central de análisis de este trabajo, parece que lo más conveniente sea evitar solapamientos de las normas, además de tratar de simplificar el marco legal[52].

Por otro lado, quisiera llamar la atención sobre el hecho constatado de que la datificación de unas elecciones implica la aplicación de normas comunitarias que afectan a una multitud de aspectos. Por ejemplo, en nuestro ámbito obsérvese que habrá que aplicar también normativa comunitaria que excede a lo que se pretende en la norma sectorial. Buen ejemplo de lo que decimos lo constituyen las múltiples variables que presentan los ciberataques a las elecciones en cualquiera de sus fases procedimentales y, más concretamente, en los momentos claves del proceso electoral (campaña electoral, día de reflexión, sistemas de votación, etc.). Por no hablar de los ataques informáticos a las infraestructuras de los partidos políticos, a

[49] Enmienda considerando 56.

[50] COM (2021) 734 final, 2021/0375 (COD) de 25. 11.2021.

[51] Dictamen 01/2022, sobre la propuesta de la Comisión de Reglamento sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones política europeas, aparatado 45: 17. Este Dictamen está disponible en:

(https://www.eca.europa.eu/Lists/ECADocuments/OP22_01/OP_EU-political-parties-and-foundations_ES.pdf).

[52] En idéntico sentido se pronuncia el Tribunal de Cuentas Europeo en el Dictamen 1/2022, p.19.

CC BY SA

DOI: https://doi.org/10.51915/ret.307

la de los candidatos que concurren en el proceso electoral o a la de las autoridades públicas que organizan o controlan la integridad de los procesos electorales. En esta línea, no sería en absoluto descartable, más bien lo contrario, que haya que trasponer y aplicar la Directiva 2022/2555 del Parlamento europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) núm. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Porque no se olvide que, tal y como y como recoge el Considerando 31 de esta directiva, las entidades pertenecientes al sector de las infraestructuras digitales se basan esencialmente en sistemas de redes y de información, por lo que las obligaciones impuestas a dichas entidades en virtud de la presente Directiva deben abordar de manera exhaustiva la seguridad física de dichos sistemas como parte de sus medidas para la gestión de los riesgos de ciberseguridad y obligaciones de notificación. Sin duda, las vulnerabilidades que presentan los sistemas de redes y de información pueden causar un gravísimo daño en el entorno digital, y la reducción de los riesgos resulta un elemento central para evitar daños.

En ese salto al vacío de la manipulación de unas elecciones por enemigos internos o externos es en el sistema de garantías coordinado y bien definido de quienes garantizan la transparencia en integridad del proceso electoral y de las autoridades de protección de datos, donde debe dirigirse la atención normativa. Un enfoque sobre la gestión de riesgos en cada proceso electoral llevado a cabo por un equipo multidisciplinar debe ser una obligación perentoria. Obviamente, en el mismo se deben reflejar aquellos elementos que situando en el centro ese concreto proceso electoral pongan en peligro la seguridad nacional.

El RGPD se aplica en las elecciones, ya sean nacionales, ya sean europeas, y se aplica a quienes concurren en el proceso electoral, a los partidos políticos, a las agrupaciones electorales, a las coaliciones electorales, a los candidatos y las candidatas, a las autoridades públicas, a los responsables del proceso electoral y a quienes controlan el proceso electoral, a los analistas de datos, a las plataformas de redes sociales y de redes de publicidad en línea y a todos aquellos que pueden poner en peligro el sistema por un uso ilegítimo de los mismos durante las elecciones. Como bien ha expresado la Comisión, "prácticamente todas las operaciones de tratamiento de datos en el contexto electoral están sujetas al RGPD". No obstante, a mi juicio, se debe prestar una atención preeminente y multinivel a un sistema de garantías reforzado que exige la protección de los datos personales como elemento nuclear sobre el que descansa unas elecciones democráticas en el entorno digital.

Quiero concluir con una idea clave, reiterada en diversos trabajos, pero en este caso lo haré con la expresión del SEPD en su Dictamen 3/2018: "El problema es real y

CC BY SA

DOI: https://doi.org/10.51915/ret.307

urgente, y es probable que empeore a medida que más personas y las cosas se conectan a internet y aumenta el papel de los sistemas de Inteligencia Artificial"[53]. En efecto, la protección de datos es quizás la mayor parte de la solución, mucho más de lo que a veces podemos llegar a imaginar.

Resulta completamente ingenuo confiar en los propósitos de las tecnológicas y en la capacidad de autorregulación sobre algunas de las cuestiones que se ha planteado con la regulación. Baste recordar la campaña iniciada por Google frente a la propuesta de Reglamento, campaña que parece articularse a través de las ONGs y los yotubers. Según los medios de comunicación, Google ha enviado cartas a los europarlamentarios advirtiendo de que el ejercicio de la libre expresión política de los ciudadanos en las redes podría terminar tratándose como las campañas pagadas por partidos en las grandes plataformas digitales. Sin ir más lejos, el pasado 13 de marzo de 2023, tras la votación a favor de la propuesta de Reglamento en el Plenario del Parlamento Europeo (2 de febrero), las asociaciones Ametic y Adigital advertían que "la nueva propuesta de Reglamento Europeo sobre anuncios políticos podrían debilitar el funcionamiento democrático de la Unión Europea y los Estados miembros" [54] y solicitaban a los legisladores participantes a valorar los efectos tanto directos como colaterales de la propuesta realizando un llamamiento a las instituciones europeas a rectificar a tiempo la regulación de los anuncios políticos[55].

En mi opinión, no conviene confiar en los códigos de buenas prácticas ni en la autorregulación empresarial, no digamos de las grandes tecnológicas, como medio eficaz, efectivo y en buena parte suficiente para garantizar los derechos en juego de los ciudadanos. Por citar el ejemplo del Código de Buenas prácticas en materia de desinformación de 2018, que son normas de autorregulación para luchar contra la desinformación, que se ha tenido que reforzar en 2022, siguiendo las recomendaciones de la Comisión de mayo de 2021[56]. Obsérvese que en materia de transparencia de la publicidad política este código reforzado "compromete" a los signatarios a aplicar medidas de transparencia más estrictas "permitiendo a los usuarios a reconocer fácilmente los anuncios políticos proporcionando un etiquetado más eficiente comprometiéndose a revelar el patrocinador, el gasto publicitario y el período de visualización. Además, los firmantes se comprometen a

[53] Opinion 3/2018, EDPS Opinion online manipulation and personal data: 22.

[54] Tal y como se denunciaba en la página de Ametic la voz de la Industria Digital (ametic.es).

[55] Véase el documento "Llamamiento de las asociaciones digitales a las Instituciones Europeas a rectificar a tiempo la regulación sobre anuncios políticos". Este documento se puede consultar en el enlace https://ametic.es.

[56] El Código de Buenas Prácticas en materia de Desinformación reforzado de 2022 se puede consultar en el siguiente enlace: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

CC BY SA

DOI: https://doi.org/10.51915/ret.307

poner en marcha bibliotecas publicitarias eficientes y con capacidad de búsqueda para la publicidad política"[57].

Bibliografía

Arenas Ramiro, M. 2019. "Partidos políticos, opiniones políticas e Internet", *Teoría y Realidad Constitucional*, núm. 44: 341-372.

García Sanz, R.M. 2019. "Tratamiento de datos personales de las opiniones políticas en el marco electoral: Todo en interés público". *Revista de Derecho Político*, núm. 183: 129-159.

Garriga Domínguez, A. 2020. "Reflexiones sobre el marketing político y el fenómeno de la desinformación en el contexto electoral". *Anuario de Filosofía del Derecho*: 251-287.

García Mahamut, R.:

- 2015. "Elecciones y protección de datos: los grandes desafíos para la UE" en Rallo Lombarte y García Mahamut (edts.) *Hacia un nuevo derecho europeo de protección de datos*, Valencia,Tirant lo Blanch.

-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: 309-338.

Gibson, R. & Ward, S. 2009. "Parties in the Digital age — a review article". *Representation* vol. 1, núm. 45: 87-100.

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: 41-73.

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.

Kefford, G., Dommett, K. y Rzepecki, E. 2022. "Data-driven campaigning and democratic disruption: Evidence from six advanced democracies". Sage Journals, Vol. 29, n.3., 2022, https://doi.org/10.1177/13540688221084039.

Latimer, Ch.P. 2008. "Utilizing the Internet as a Campaign Tool: The Relationship Between Incumbency, Political Party Affiliation, Election Outcomes, and the

[57] Ibidem.

CC BY SA

DOI: https://doi.org/10.51915/ret.307

Quality of Campaign Web sites in the United States". *Journal of Information Technology & Politics,* 4:3 81-95.

Pauner Chulvi, C. 2022. "Sobre la compleja relación entre los medios de comunicación y las plataformas tecnológicas. Google news y los derechos de autor en el entorno digital". *Revista de Derecho Político*, núm. 115: 43-72.

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.

Serra Cristóbal, R. 2023 "Noticias falsas y derecho a recibir información veraz. Dónde se fundamenta la posibilidad de controlar la desinformación y cómo hacerlo". *Revista de Derecho Político*, núm. 116: 13-46.

Viguri Cordero, J. 2021. La adopción de instrumentos de certificación como garantía eficiente en la protección de los datos personales. *Revista Catalana de Dret Públic*, núm. 62: 160-176

.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

Transparencia algorítmica en los medios de comunicación y las plataformas digitales

Cristina Pauner Chulvi[1]

Catedrática de Derecho Constitucional

Universitat Jaume I de Castellón
España
ORCID: 0000-0003-2863-0664

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

El presente trabajo se enmarca en el proyecto de investigación DATATRANSCO con referencia nº PID2021-128309NB-I00 del Ministerio de Ciencia, Innovación y Universidades.

RESUMEN: La transparencia algorítmica ha cobrado especial relevancia en el contexto de la información y la comunicación porque la utilización de algoritmos en medios de comunicación y plataformas está absolutamente extendida e integrada en todos sus aspectos. La falta de transparencia sobre el uso de estas herramientas matemáticas unida a las características intrínsecas de los algoritmos ha provocado efectos negativos en el contexto del periodismo como la dificultad de cumplir con su función de perro guardián y de las plataformas contribuyendo a la difusión de desinformación, la censura de contenidos o la explotación ilegal de datos. Por ello, las disposiciones que está adoptando la Unión Europea en materia de transparencia algorítmica constituyen un avance para mitigar los riesgos de la manipulación informativa y garantizar los derechos de los usuarios.

PALABRAS CLAVE: Algoritmos, transparencia algorítmica, inteligencia artificial, medios de comunicación, redes sociales, plataformas tecnológicas, explicabilidad.

[1] Catedrática de Derecho Constitucional en la Universitat Jaume I. Sus líneas de investigación actuales están centradas en las libertades de expresión e información, protección de datos personales y transparencia. Es autora de numerosos artículos en revistas especializadas y sus más recientes publicaciones versan sobre desinformación y noticias falsas, protección de datos y periodismo y plataformas tecnológicas y derechos de autor.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

CONTENIDOS: 1.-Introducción. 2.-La gestión algorítmica de la información llevada a cabo por los medios de comunicación tradicionales. *2.1.-La transformación digital en los medios de comunicación. 2.2.-Los retos de los algoritmos en las redacciones informativas. 2.3.-El periodismo digital y la función de perro guardián de la democracia.* 3.-Los algoritmos en las plataformas tecnológicas. 4.-Transparencia algorítmica: los elementos clave de los algoritmos que determinan la creación y difusión de información. 5.-La transparencia algorítmica en la producción de la Unión Europea y su aplicación a los medios de comunicación y plataformas tecnológicas. 6.-Conclusiones. -Bibliografía.

Algorithmic transparency in media and digital platforms

ABSTRACT: Algorithmic transparency has gained special relevance in the context of information and communication because the use of algorithms in the media and platforms is absolutely widespread and integrated in all its aspects. The lack of transparency about the use of these mathematical tools together with the intrinsic characteristics of the algorithms have lead to negative effects in the context of journalism, such as the difficulty of fulfilling its function as watchdog and of the platforms contributing to the spread of disinformation, the censorship of content or the illegal exploitation of data. For this reason, the provisions that the European Union is adopting in terms of algorithmic transparency constitute progress in mitigating the risks of information manipulation and guaranteeing the rights of users.

KEYWORDS: Algorithms, algorithmic transparency, artificial intelligence, media, social networks, technology platforms, explainability.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.308

1.- Introducción

El término "transparencia" recoge múltiples acepciones y se aplica en contextos muy diferentes (corrupción, desarrollo económico, regulación de los mercados, economía política, protección ambiental, etc.), aunque ha adquirido gran protagonismo en relación con todas las ciencias vinculadas con el desarrollo de los algoritmos. La transparencia algorítmica puede definirse brevemente como la divulgación de información sobre algoritmos para permitir su supervisión, comprobación, o intervención por parte de cualquier persona interesada[2].

Este interés por garantizar la transparencia algorítmica alcanza al contexto de la información y la comunicación porque la utilización de algoritmos en medios y plataformas está absolutamente extendida e integrada en todos sus aspectos.

Aplicados al periodismo, los algoritmos pueden utilizarse para jerarquizar, clasificar y filtrar información; para medir las audiencias, para determinar temas que cubrir y para escribir historias. Se trata de la creación de contenidos a gran escala, personalizándolos a las necesidades de cada lector individual y sin necesidad de intervención humana. Es el periodismo automatizado que combina el uso de *big data* y los más complejos sistemas algorítmicos, especialmente, la inteligencia artificial (IA en adelante) en las fases de recopilación y distribución de noticias y, cada vez más, en la fase de redacción[3].

Los algoritmos son asimismo elementos nucleares para el funcionamiento de las plataformas digitales en las que se editan, publican e intercambian contenidos creados por los propios usuarios o terceros. Las redes sociales emplean algoritmos y sistemas de IA para la moderación de contenido (búsqueda y detección de contenido inapropiado), el *ranking* de contenido (organizar, clasificar y presentar el contenido generado por el usuario), el *targeting* de contenido (promocionar a terceros los contenidos comerciales no solicitados) y la creación de influencia social (influir en el desarrollo de las redes sociales de cada usuario mediante recomendaciones sociales).

---

[2] Un completo análisis del concepto de transparencia algorítmica en COTINO HUESO, L. 2022. "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta", en *Transparencia y explicabilidad de la Inteligencia Artificial.* Tirant lo Blanch: Valencia, pp. 25-69.

[3] Carlson define el periodismo automatizado como "los procesos algorítmicos que convierten datos en textos informativos narrativos con intervención humana limitada o nula más allá de las opciones de programación iniciales" [CARLSON, M. 2014. "The robotic reporter: automated journalism and the redefinition of labor, compositional forms and journalistic authority". *Digital Journalism,* vol. 3(3): 416-431].

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.308

Toda esta actividad se basa en la explotación de los macrodatos que, de forma voluntaria o inconsciente, los usuarios facilitan a las plataformas así como el análisis de la información que las plataformas tecnológicas son capaces de detectar –desde la ubicación y estado de ánimo del consumidor a la actividad que desarrolla mientras está consumiendo contenido– de suerte que es posible crear un ADN digital integral para los usuarios a fin de dirigirles de manera automática contenido y publicidad en función de sus perfiles digitales[4].

Puede imaginarse que el empleo de algoritmos en la producción de una noticia tiene consecuencias muy distintas al uso de estas herramientas matemáticas para realizar la selección de noticias que el usuario va a recibir en sus redes sociales por lo que las condiciones de transparencia que el ordenamiento jurídico les impone son distintas. Pero, en cualquier caso, la transparencia sobre su funcionamiento sirve a objetivos de primer orden en un Estado democrático de Derecho: en el caso de los medios tradicionales que automatizan tareas como la redacción de noticias o prestan atención a sus usuarios a través de chatbots, la transparencia sirve principalmente a la comprobación de la veracidad de la información y se convierte en una cuestión clave para la ética periodística. En el caso de las plataformas, la transparencia en el uso de algoritmos sirve a la defensa de derechos fundamentales de las personas tales como el derecho a la protección de datos, la libertad de información y también a la protección de sus derechos como consumidores.

Efectivamente, desde hace tiempo la transparencia se ha incorporado como un valor ético clave para el periodismo considerándose como el remedio para recuperar una credibilidad y confianza de la audiencia que se había ido erosionando peligrosamente en las últimas décadas[5]. Paralelamente, las plataformas han ido aceptando progresivamente una mayor apertura sobre su funcionamiento sobre la base de protocolos y códigos de conducta, mecanismos de *soft law* que les conducen a un ejercicio voluntario de rendición de cuentas sobre la actuación de sus algoritmos en la selección (y, por tanto, también eliminación) de contenidos.

[4] LATAR, N. L. 2015. "The Robotic Journalist in The Age of Social Physics: The End of Human Journalism?", in G. Einav (ed.), *The New World of Transition Media*. Springer International Publishing: Swiss, pp. 65-80.

[5] CASERO-RIPOLLES, A. 2014. "La pérdida de valor de la información periodística: causas y consecuencias". *Anuario ThinkEPI*, núm. 8: 256-259; KOLISKA, M. 2022. "Trust and journalistic transparency online". *Journalism Studies*, vol. 23, núm. 12: 1488-1509 y BLUMLER, J. G. 2018. "The Crisis of Public Communication, 1995-2017", *Javnost-The Public*, vol. 25, núm. 1-2: 83-92. Un resumen sobre las casusas de la crisis estructural del periodismo en GARCÍA-GORDILLO, M. M.; PALAU-SAMPIO, D.; RIVAS-DE-ROCA, R. 2022. "Pero ¿qué me cuentas? Una revisión del concepto de verdad en el siglo XXI", en Caro-González, F. J.; Garrido-Lora, M.; García-Gordillo, M. M. (eds.), *El problema de la verdad. Retos y riesgos en la comunicación*. Comunicación Social Ediciones y Publicaciones: Salamanca, p. 69.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.308

No obstante, este ejercicio de transparencia basado en razones éticas o en compromisos voluntarios da lugar a una situación que no permite una evaluación completa para determinar si medios de comunicación y plataformas están respetando sus obligaciones. Por ello, también a ambas ha alcanzado la normativa europea porque, en la actualidad, al margen de esa naturaleza ética, la transparencia es un estándar jurídico impuesto en regulaciones que afectan a estas entidades.

En las líneas que siguen nos ocuparemos de analizar, en primer lugar, el impacto de la transformación digital en los medios de comunicación y el reto que plantea la gestión algorítmica de la información en las redacciones; en el siguiente apartado nos centramos en las funciones de las plataformas digitales en el ecosistema de la información pública y los efectos problemáticos del uso de algoritmos en esas actividades lo que nos llevará a la reflexión sobre el fenómeno de la desinformación. A continuación, abordaremos la noción de transparencia algorítmica y los elementos clave que deben conocerse sobre los algoritmos porque son los que determinan la creación y difusión de información. Seguidamente, nos ocuparemos de exponer las más recientes normativas europeas en las que se consagra la transparencia algorítmica, concretamente, el futuro Reglamento de Inteligencia Artificial y el Reglamento de Servicios Digitales. El estudio se cierra con unas conclusiones finales.

2.- La gestión algorítmica de la información llevada a cabo por los medios de comunicación tradicionales

2.1.- La transformación digital en los medios de comunicación

Con carácter general, se afirma que el periodismo es una actividad sujeta al impacto de las novedades tecnológicas y "cada nueva oleada multiplica las posibilidades, crea nuevos modelos de negocio y afecta a la relación entre el periodista y la audiencia"[6]. Herramientas como los drones, el *blockchain*, los algoritmos o los chatbots, entre otros muchos, forman parte de un cambio cultural que ha conducido al periodismo digital[7] que ampara todas las formas de periodismo que recurren a recursos digitales y en el que los profesionales de la información utilizan masivamente la tecnología, un recurso cuyo último reto es la llegada de la inteligencia artificial.

En realidad, los medios de comunicación tradicionales han padecido enormemente la revolución digital porque supuso una transformación radical de su mercado

[6] MANFREDI SÁNCHEZ, J. L. y UFARTE RUÍZ, M. M. 2020. "Inteligencia artificial y periodismo: una herramienta contra la desinformación*. *Revista CIDOB d'Afers Internacionals*, núm. 124: 50.

[7] Como indica Salaverria, no es posible recopilar las múltiples denominaciones acuñadas para referirnos al ciberperiodismo, periodismo online, periodismo de alta tecnología, periodismo multimedia o incluso robot periodismo (SALAVERRÍA, R. 2019. "Digital journalism: 25 years of research. Review article". *El profesional de la información*, vol. 28, núm. 1).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

debido, en primer lugar, a un cambio en el modelo de negocio de la comunicación cuyos ingresos se basaban principalmente en la explotación de la publicidad, beneficios que ahora se desvían hacia las plataformas tecnológicas (Facebook, Google…) convertidas en las intermediarias en el mundo de la información.

Pero también y en segundo término, por la ruptura del proceso de comunicación que dejaba de estar controlado por unos emisores – los medios – que difundían la información y noticias a los receptores – la ciudadanía – con un control absoluto sobre la forma, la selección de contenido y el alcance de esa información.

La apertura del entorno digital a una comunicación global e ininterrumpida en la que basta con disponer de un ordenador y de conexión a Internet, convirtió a cualquier persona en una potencial comunicadora y receptora, a su vez, de contenidos. Aparecieron medios digitales nativos y medios digitales ligados a marcas periodísticas tradicionales (*legacy media*), surgió la participación activa de los ciudadanos en la comunicación pública mediante elaboración y diseminación de contenidos elaborados por los propios usuarios (*crowdsourcing*), la relación con el receptor se tornó bidireccional abriéndose espacios en los medios para los comentarios, colaboraciones y contribuciones informativas por parte de la audiencia y la reconfiguración interna de las compañías fue absolutamente radical obligando a nuevas estrategias de innovación y la adaptación de sus profesionales a los nuevos formatos, lenguajes y géneros en la era de la información digital.

Así, entre 2009 y 2012, los medios de comunicación se volcaron en el diseño de modelos informativos basados en datos masivos (*big data* o macrodatos) y en el desarrollo y uso de algoritmos que les permiten explotar nuevas formas de crear y difundir contenidos[8]. En el escenario actual, estos procesos están totalmente consolidados y en las redacciones digitales se emplean los potentes y complejos algoritmos de IA para la automatización de la recogida y documentación de información, la producción automatizada de contenido, la distribución de información y la relación con la audiencia. Por tanto, estas herramientas algorítmicas ya están disponibles para todo el proceso periodístico.

En el debate sobre el uso de algoritmos en los medios de comunicación, la visión optimista se centra en el ahorro de tiempo, la elaboración de contenidos en múltiples

[8] Se señala 2014 como el momento que marcó el arranque definitivo de la inteligencia artificial en el periodismo cuando *Los Angeles Times* publicó una noticia sobre movimientos sísmicos elaborada por el software Quakebot (SALAVERRÍA, R. 2014. "Periodismo en 2014: balance y tendencia". *Cuaderno de Periodistas*, núm. 29: 19). Sobre el tema, véanse entre otros ELÍAS, C. 2015. *Big data y periodismo en la sociedad red*. Editorial Síntesis: Madrid; SALAZAR, I. 2018. "Los robots y la Inteligencia Artificial. Nuevos retos del periodismo", *Doxa Comunicación,* núm. 27: 295-315 y FLORES-VIVAR, J. M. 2018. "Algoritmos, aplicaciones y Big data, nuevos paradigmas en el proceso de comunicación y de enseñanza-aprendizaje del periodismo de datos". *Revista de Comunicación*, vol. 17, núm. 2: 268-291.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

idiomas, la prevención frente a errores y sesgos y, especialmente, en la oportunidad que supone para los profesionales de la información a quienes descargarán de tareas repetitivas permitiendo concentrarse en trabajos de investigación más profundos lo que puede redundar, en última instancia, en el estado del periodismo profesional y contribuir al incremento de la calidad periodística[9].

La visión pesimista o crítica, por el contrario, prevé una desaparición de puestos de empleo con la sustitución de periodistas humanos por robots; denuncia una serie de limitaciones de la IA relacionadas con las características de los algoritmos que pueden impactar negativamente en derechos y libertades (sesgos, opacidad, discriminación,…) pero muy destacadamente, señala la ineptitud de los algoritmos para cumplir con la función de "perro guardián" que se asigna al periodismo en el Estado democrático de Derecho en su tarea de supervisar el funcionamiento de los gobiernos y la sociedad[10]. Por lo tanto, nunca pueden "convertirse en guardianes de la democracia y los derechos humanos"[11]. Nos detendremos en el análisis de estos argumentos.

2.2.- Los retos de los algoritmos en las redacciones informativas

La preocupación más extendida entre la profesión periodística es la de que se utilice este tipo de automatismos para escribir noticias y cualquier otro tipo de contenido por el riesgo de que se sustituyan rápidamente a los periodistas humanos por robots. Sin embargo, el primer estudio académico centrado en el desarrollo tecnológico

[9] Por todos, véase VAN DALEN, A. 2012. "The algorithms behind the headlines". *Journalism Practice*, vol. 6, issue 5-6: 648-658. Wölker y Powell plantean una adaptación ideal de periodismo combinado, ya que fusiona la capacidad del periodista humano de escribir e interpretar creativamente con el potencial de los algoritmos para hacerse cargo de las tareas rutinarias (WÖLKER, A. & POWELL, T. E. 2018. "Algorithms in the newsroom? News readers'perceived credibility and selection of automated journalism". *Journalism,* vol. 22, issue 1: 99-100).

[10] La doctrina que permite atribuir a la prensa su papel de perro guardián de las libertades está avalada por los tribunales nacionales e internacionales desde la famosa sentencia del Tribunal Supremo norteamericano en el caso *Sullivan* (*New York Times Co. v. Sullivan*, de 9 de marzo de 1964). hasta los numerosos casos resueltos por el TEDH (por todas, SSTEDH de 15 de febrero de 2005, asunto *Steel y Morris c. Reino Unido*; 16 de julio de 2003, asunto *Wegrzynowski y Smolczewski c. Polonia;* 10 de marzo de 2009, asunto *Times Newspapers Ltd c. Reino Unido*; y 9 de marzo de 2021, asunto *Benítez Moriana e Íñigo Fernández c. España),* y pasando por los pronunciamientos de nuestro Tribunal Constitucional a partir de su primera sentencia sobre libertad de información (STC 6/1981, de 16 de marzo). La bibliografía sobre este tema resulta inabarcable por lo que nos limitamos a recomendar a VILLAVERDE MENÉNDEZ, I. 2004. *Estado democrático e información: el derecho a ser informado*, Junta General del Principado de Asturias: Oviedo y ALBERTOS, J. L. M. 1994. "La tesis del perro-guardián: revisión de una teoría clásica". *Estudios sobre el mensaje periodístico,* núm. 1: 13-25.

[11] WÖLKER, A. & POWELL, T. E. 2018. "Algorithms in the newsroom? …" *cit.,* pp. 86-103,

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.308

español de inteligencia artificial en periodismo concluye que la producción automatizada de noticias queda relegada a un segundo plano y predomina el uso de algoritmos y sistemas automatizados en las fases de recogida de información y de distribución de contenido relacionada con la monetización[12].

Y precisamente esta búsqueda de la finalidad lucrativa como interés superior es el que puede desvirtuar la labor del periodista apartándolo de la búsqueda por cubrir asuntos de interés público. Los sitios web en los que se publican las noticias tienen la capacidad de medir con precisión el índice de lectura de los artículos por lo que esta información puede ejercer una enorme presión sobre el periodista para ajustar el contenido de cada una de sus publicaciones en la competencia por la atención de los consumidores[13].

La capacidad de enviar contenido directa y velozmente a los consumidores en función de sus perfiles sitúa al periodismo robot en una situación de ventaja significativa frente al periodista humano pero implica la búsqueda de una eficiencia económica que, siendo legítima, reduce al ciudadano a la condición de consumidor y promueve el marketing emocional porque aplica al periodismo métodos de investigación social y de comportamiento a través de la exploración profunda de bases de datos, encuestas, y una combinación general de informática y ciencias sociales[14].

Por otra parte, sobre los algoritmos de IA pesan algunas limitaciones serias porque los algoritmos de minería de datos son capaces de descubrir nuevas conexiones entre múltiples variables gracias a la gran cantidad de datos que analizan, pero las conclusiones que extraen de estos descubrimientos pueden ser falsas bien porque los datos que los nutren son erróneos o porque su programación es incorrecta ya sea por inferencias defectuosas del diseño o porque el programador introdujo sesgos.

Además, estos sistemas de algoritmos tan avanzados producen textos coherentes, gramaticalmente correctos y hasta elocuentes con una persuasiva impresión de razonamiento gracias a la optimización de sus modelos lingüísticos. Pero coherencia no es sinónimo de verdad lo que nos aboca al problema de las noticias falsas que alcanzan después una difusión imparable a causa de la viralidad con la que se difunden en las redes sociales. Incluso las IA más avanzadas no comprenden, por el

[12] SÁNCHEZ-GARCÍA, P.; MERAVO-ÁLVAREZ, N.; CALVO-BARBERO, C. y DIEZ-GRACIA, A. 2023. "Desarrollo tecnológico español de la inteligencia artificial aplicada al periodismo: empresas y herramientas de documentación, producción y distribución de información". *Profesional de la Información*, vol, 32, núm. 2.

[13] MÉNDEZ, L. 2021. "El algoritmo sustituye al periodismo". *Cuadernos de Periodistas*, núm. 42: 65-70.

[14] MEYER, P. 1975. "Precision journalism". *Communication Information*, vol. 1, núm. 1: 164-165.

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

momento, la diferencia entre verdadero y falso ni el sentido ni significado de términos o palabras.

Otra limitación de los algoritmos se relaciona con la exigencia ética del periodismo mediático de la separación entre hechos y opiniones**.** La ética del periodismo robótico aún no se ha escrito pero, afortunadamente, hay regulación que ya obliga a las editoriales a informar al lector si una historia fue escrita por un robot o por un periodista humano. Aunque existe algún experimento, los algoritmos carecen de la capacidad de escribir opiniones ya que pueden proporcionar nuevos conocimientos, pero no pueden integrar esos nuevos conocimientos en sugerencias de políticas o cambios. También se ha señalado que los algoritmos no pueden hacer preguntas, sino que solo pueden intentar responderlas**,** un inconveniente que desafía una pauta básica del ejercicio periodístico.

La doctrina ha apuntado otras limitaciones de la IA relacionadas con la capacidad de sus complejos algoritmos para comprender el lenguaje natural humano, especialmente el contexto de las ideas, las metáforas, el humor y la poesía[15]**.** La importancia de estos elementos (contexto, intencionalidad, tono) a la hora de construir un relato es difícil de exagerar y se tienen en cuenta a la hora de otorgar protección constitucional a periodistas en el ejercicio de su libertad de expresión. Así, la comprensión del lenguaje natural por parte de la IA no puede ir más allá de un proceso burocrático, que actúa según unas estrictas reglas mecánicas de forma que un periodista robot nunca podrá "escribir" historias cuya profundidad y riqueza vayan más allá del "nivel burocrático" que le puede dar el periodista humano, que puede ser empático y puede comprender contextos culturales complejos.

2.3.- El periodismo digital y la función de perro guardián de la democracia

Algunas de estas limitaciones están superadas o van a serlo en breve por los veloces avances que ha experimentado la IA en los últimos años. Sin embargo, aunque el periodismo automatizado evolucionara en sofisticación persiste una gran debilidad: las computadoras nunca actuarán como el cuarto poder, ejerciendo esa función de vigilancia independiente del poder asignada al periodismo**.**

El periodismo y la democracia están vinculados a través de un "contrato social", donde los periodistas asumen el papel de guardianes de los políticos y la sociedad para no abusar de su autoridad[16]. Desde esta perspectiva, los medios y el periodismo necesitan democracia porque es la única forma de gobierno que respeta la libertad

[15] LATAR, N. L. 2015. "The Robotic Journalist in The Age of Social Physics…?", *cit*., pp. 76-77.

[16] STRÖMBACK, J. 2005. "In Search of a Standard: four models of democracy and their normative implications for journalism". *Journalism Studies*, vol. 6(3): 332.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

de expresión y de información y la independencia de los medios de comunicación respecto del Estado.

A su vez, la democracia requiere de un sistema de flujo de información para la discusión pública[17]. Aquí es donde entran en escena los medios y el periodismo porque proporcionan a los ciudadanos la información que requieren para ser libres y autónomos[18]; facilitan al gobierno la información que necesita para tomar decisiones en interés común y valorar el impacto que su gestión política causa en la ciudadanía; proveyendo de una arena para la discusión pública y actuando como un perro guardián contra el abuso de poder en la política y en otras partes de la sociedad.

Desde el punto de vista constitucional, esta última cuestión es nuclear. Así, en primer lugar, el hecho de que la noticia no sea creada por un profesional de la información puede provocar dudas respecto al cumplimiento del famoso estándar de diligencia profesional que sirve a la hora de evaluar la veracidad de la información de la que depende, en última instancia, que la información goce o no de protección constitucional. Como sabemos, la Constitución reconoce en su artículo 20.1.d) el derecho a recibir información veraz y el Tribunal Constitucional ha determinado, en una línea jurisprudencial invariable, que veracidad no equivale a verdad, sino que implica que una noticia ha sido elaborada ajustándose a los cánones del buen profesional del periodismo como la práctica del análisis de la calidad de las fuentes (tipo, diversidad e identificación de la fuente), el contraste y verificación de la información, etc. Asimismo, exige una serie de competencias y habilidades profesionales como la calidad en la redacción y el manejo del idioma.

Como resumen Manfredi y Ufarte, "El criterio periodístico distingue qué asuntos son relevantes y las noticias se articulan para explicar lo que sucede de acuerdo con una cierta idea de objetividad, que se complementa con la opinión y la interpretación analítica. La condición de veracidad subyace así en la calidad del texto, por lo que esta puede reclamarse tanto en las piezas informativas como en las opinativas. Ello permite al lector reconocer un texto periodístico de calidad frente a un rumor: se cita la fuente, el periodista está presente, se evita el uso del condicional, además de otras características habituales en la definición del valor periodístico"[19].

---

[17] Como Carey argumentó célebremente "Sin periodismo no hay democracia, pero sin democracia tampoco hay periodismo'' (CAREY, J. 1996. Where journalism education went wrong. *Presentation at the Middle Tennessee State University).*

[18] KOVACH, B. & ROSENSTIEL, T. 2001. The elements of journalism. What news people should know and the public should expect. Three Rivers Press: New York, p. 12,

[19] MANFREDI SÁNCHEZ, J. L. y UFARTE RUÍZ, M. M. 2020. "Inteligencia artificial y periodismo…, *cit.,* p. 54.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.308

Por el contrario, "las noticias promovidas a través de algoritmos representan un periodismo en el que la intervención humana puede darse solo en instancias ajenas al propio proceso periodístico, ya que se limita al diseño del algoritmo por ingenieros informáticos y al diseño y creación de bases de datos y de las plantillas de redacción"[20]. Esto nos aboca al problema de la implicación de los algoritmos en la posible generación de relatos falsos o *fake news* que afecta profundamente a la condición del periodismo como foro público donde se alienta el debate y la discusión presidida por la reflexión y la convivencia. Una esfera pública, inclusiva y estructurada hasta ahora, que ha quebrado y ha pasado a ser una esfera disruptiva y radicalizada por la relevancia de medios no tradicionales y digitales y la irrupción de las plataformas.

En segundo lugar, los sistemas algorítmicos de IA tienen limitaciones para construir razonamientos críticos y emitir opiniones sobre cuestiones sociales o políticas lo que los invalida en esta función de controladores de la acción de gobierno. Este papel de perro guardián antes de la era de los nuevos medios se llevó a cabo, mayoritariamente, por periodistas cualificados que se centraban en descubrir los hechos que rodeaban a las transgresiones políticas graves (caso *Watergate*, el caso *Boston Globe* o los papeles de Panamá son referencias reveladoras). Este tipo de periodismo no es posible abordarlo únicamente con las herramientas actuales de construcción de noticias en las redacciones digitales que todavía se centran en elaborar información financiera, meteorológica, deportiva o de servicios, temas repetitivos para los que se dispone de datos limpios, precisos y estructurados aunque este listado de generación automatizada de información se amplía sin parar.

Es indiscutible que los recursos tecnológicos han facilitado la labor de rastreo, recopilación y análisis de la información, lo que en principio potencia la capacidad de los periodistas para cumplir con su papel de vigilantes, pero existen aspectos del papel de guardián de las instituciones que se han vuelto imposibles de satisfacer en la era del periodismo digital y plantean cuestiones serias para el discurso democrático. Básicamente, por la cuestionable calidad de buena parte de la información: en la era de los nuevos medios de comunicación, muchas noticias consisten en la cobertura de un número inacabable de escándalos llamativos (ya sean reales, exagerados o completamente inventados) que frecuentemente solo están relacionados tangencialmente con el gobierno. Estas controversias artificiosas y pequeñas informaciones triviales explotadas y reproducidas con fines

[20] TÚÑEZ-LÓPEZ, M.; TOURAL-BRAN, C. y VALDIVIEZO-ABAD, C. 2019. "Automatización, bots y algoritmos en la redacción de noticias. Impacto y calidad del periodismo artificial", *Revista Latina de Comunicación Social*, núm. 74: 1414.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

sensacionalistas apenas dejan espacio para la cobertura de asuntos relevantes relacionados con la política o la gobernanza[21].

Finalmente, tampoco sirve bien a la función de perro guardián que se utilicen algoritmos en las redacciones con el objeto de personalizar las recomendaciones de contenido en función de los intereses y preferencias de los lectores. Una estrategia propia de las redes sociales y que resulta más problemática e intensa para los medios de comunicación porque "puede entrar en contradicción con la misión democrática periodística de contribuir a la conversación comunitaria en torno a temas de interés público y de proporcionar a la ciudadanía espacios comunes que le faciliten desarrollar criterios sólidos para tomar decisiones políticas informadas"[22].

Por lo tanto, se abre un debate ético y jurídico complejo sobre el periodismo artificial y sus efectos en el público que debe conservar indemnes las garantías de sus derechos. Hay que mantener el papel de servidor y guardián de las instituciones, la adhesión de la IA a valores éticos y, sobre todo, la rendición de cuentas para garantizar la transparencia de los algoritmos. El público tiene derecho a entender cómo se construye la información y a partir de qué datos.

3.- Los algoritmos de las plataformas tecnológicas

La irrupción de las redes sociales en el escenario de la comunicación digital marcó un punto de inflexión para los medios porque se estableció una clara competición entre ambos como fuentes de información[23]. En la actualidad, las redes sociales constituyen el principal canal de información para los usuarios que confían en ellas como fuentes de noticias en detrimento de la industria periodística que deja de ser el actor preferente para vehicular mensajes informativos. Así, los medios y plataformas mantienen una feroz competencia por captar la atención de los usuarios aunque, a su vez, establecen una relación de dependencia en la que los medios facilitan contenidos a las redes que, a su vez, los dotan de visibilidad[24].

---

[21] OWEN, D. 2018. "El papel de los nuevos medios en la política", en *La era de la perplejidad. Repensar el mundo que conocíamos.* Taurus: Barcelona.

[22] VENTURA POCINO, P. 2021. Algoritmos en las redacciones: Retos y recomendaciones para dotar a la inteligencia artificial de los valores éticos del periodismo. Consell de la Informació de Catalunya, p. 23.

[23] Sobre la relación de los medios de comunicación y las plataformas como fuentes de información, véase MAGALLÓN ROSA, R. 2021. "Medios de comunicación y redes sociales: entre el conflicto, la (in)dependencia y la colaboración". *Cuadernos de periodistas*, núm. 42: 9 y 10.

[24] MARTÍNEZ-COSTA, M. P. 2018. "El mercado de los medios digitales en España". *Cuadernos de Periodistas*, núm. 37: 82 y 83.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

En el contexto de la digitalización, las redes sociales se presentan como un escenario para el riesgo porque, junto con tantas otras innovaciones surgidas tras la aparición de Internet, son servicios prestados por las gigantes plataformas tecnológicas que los presentan "poco menos que como una benevolente prestación gratuita"[25]. Sin embargo, simbolizan el proceso de monetización de la privacidad que sujeta a los usuarios a un contrato de intercambio de servicios por información personal que se presta en un ecosistema en el que los derechos están solo débilmente garantizados.

Como ya hemos descrito en algún momento[26], los contenidos en las redes sociales son filtrados, seleccionados y organizados de manera personalizada para cada usuario. A partir de la utilización de apps, buscadores, redes sociales, etc., las personas vamos dejando un rastro de información personal que delata nuestros gustos, personalidad y preferencias. Estas interacciones son registradas por las compañías tecnológicas que customizan la información y mensajes que muestran a sus clientes con el objetivo de aumentar sus beneficios económicos puesto que el completo perfil que poseen sobre los sujetos les permite ofrecerles bienes y servicios a través de publicidad personalizada y, por lo que aquí nos interesa, eliminando contenidos e información plural y diversificada.

Los efectos de esta selección de mensajes "hecha a medida" han sido muy analizados desde que Sunstein formulara la teoría de las cámaras de eco[27] y Pariser publicara su investigación sobre los filtros burbuja[28] y si bien la doctrina no llega a conclusiones idénticas, existe un acuerdo mínimo sobre la tendencia a estar más expuestos a un determinado punto de vista, de manera que la gente ve más un tipo de contenido y se le oculta otro[29]. La combinación de este contenido personalizado, el sesgo de confirmación que reafirma a la persona en sus propios puntos de vista y el consumo en un entorno digital que nos conecta con nuestras comunidades

[25] MARTÍNEZ MARTÍNEZ, R. "Team Jorge: Desinformación, derechos fundamentales y democracia". *Agenda Pública*, 28 de febrero de 2023.

[26] PAUNER CHULVI, C. 2022. "Sobre la compleja relación entre los medios de comunicación y las plataformas tecnológicas: Google News y los derechos de autor", *Revista de Derecho Político*, núm. 115: 46.

[27] SUNSTEIN, C. R. 1999. "The Law of Group Polarization". John M. Olin Program in *Law & Economics Working Paper*, núm. 91.

[28] PARISER, E. 2011. The filter buble. What the Internet is hiding from you. Penguin Press: London.

[29] Los riesgos del contenido personalizado también se plantean para los medios de comunicación tradicionales, quizá con una intensidad mayor porque "puede entrar en contradicción con la misión democrática periodística de contribuir a la conversación comunitaria en torno a temas de interés público y de proporcionar a la ciudadanía espacios comunes que le faciliten desarrollar criterios sólidos para tomas decisiones políticas informadas" (VENTURA POCINO, P. 2021. *Algoritmos en las redacciones…,* cit. p. 23).

CC BY SA

DOI: https://doi.org/10.51915/ret.308

incentiva la viralización de contenido emocional y promueve la creación de unos estados parecidos a las mencionadas burbujas de información. El resultado es que se obtiene una lectura menos objetiva de la realidad y se debilita aquel supuesto y diverso intercambio de opiniones en el que debe sustentarse el debate en una sociedad democrática y conformarse la opinión pública.

Como mencionábamos más arriba, gran parte de los usuarios no consulta la información en las páginas web de los medios, sino que se informa a través de las redes sociales que seleccionan y ordenan algorítmicamente las noticias "afines" al consumidor. De esta forma, son las plataformas las que disponen de los datos personales de millones de usuarios, datos que ofrecen al mercado publicitario y permiten afinar al máximo la oferta para cada cliente.

Sobre los algoritmos existe una presunción de neutralidad e imparcialidad basada en el carácter objetivo que suele predicarse de las fórmulas matemáticas. Sin embargo, desde el momento en que un algoritmo se programa por una persona con una finalidad concreta, esa neutralidad desaparece. También los datos que seleccionan los algoritmos pueden estar cargados de sesgos y prejuicios que clasifican a las personas en función de estereotipos y pueden dar lugar a correlaciones falsas. Pensemos en los algoritmos predictivos o de recomendación que no analizan la persona concreta a la que está recomendando sino qué han hecho y cuáles son las preferencias de personas parecidas. Esta falta de individualización hace que, en algunos casos concretos, las predicciones del algoritmo sean erróneas: el algoritmo de recomendación de las redes sociales hace suposiciones sobre quién es más cercano o qué contenido desea ver y esas inferencias pueden no ser completamente precisas.

La complejidad de los algoritmos que emplean las plataformas puede conducir, incluso, a su inescrutabilidad por tratarse de sistemas de IA que aprenden autónomamente y obtienen deducciones inexplicables hasta para sus propios programadores. Pero esa opacidad también se debe a motivaciones empresariales que en ocasiones tienen base legal como el secreto comercial o el derecho a la protección de la propiedad intelectual pero que, asimismo, pueden ocultar una actividad poco respetuosa con los derechos fundamentales como la explotación indebida de los datos de sus usuarios o un objetivo directamente inmoral o no ético como la manipulación de la voluntad, efectos negativos en la salud mental o la difusión de noticias falsas.

Los datos y algoritmos, con apoyo del aprendizaje automático, son los que generan las técnicas sobre las que se producen estos efectos. La técnica de *manipulación activa de los contenidos* con un propósito predefinido como, por ejemplo, la manipulación electoral se produce mediante la violación de las políticas de privacidad y el manejo de datos privados por parte de la compañía tecnológica; el método de *manipulación pasiva* consiste en el refuerzo de cámaras de eco y

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

burbujas informativas que se consigue mediante la clasificación algorítmica de los usuarios de las redes en base a sus preferencias y gustos confiando en el criterio y juicio social de una caja negra de algoritmos; la táctica de *opacidad en la lógica de los algoritmos* oculta la correlación entre flujos de datos y resultados que produce el algoritmo y, por tanto, la relación causa-efecto; el recurso a las *falsificaciones audiovisuales (deepfakes)* gracias al aprendizaje de máquinas que perfeccionan imágenes falsas hasta hacerlas indistinguibles de las reales por el reconocimiento de patrones de movimientos y voz y la técnica de *creación de comunidades ficticias* que construyen un relato emocional que identifica a audiencias en las que se consigue que la emoción y sentimientos se equiparen a verdad o legalidad.

Centrándonos en la difusión viral de noticias falsas es el fenómeno que más se ve potenciado por las decisiones algorítmicas en la red constituyendo una de las principales preocupaciones sociales en el ámbito de la comunicación[30], tal y como destaca la *Declaración conjunta sobre libertad de expresión y "noticias falsas" ("Fake news"), desinformación y propaganda*[31]. Los mensajes con contenido falso se propagan rápidamente "generando un desorden informativo y constituyendo un riesgo notable para determinados valores y derechos constitucionales y para el normal funcionamiento de las propias democracias"[32], unos riesgos que se han abordado desde diversas perspectivas además de la periodística y, muy destacadamente, han entrado a formar parte de las estrategias de seguridad a nivel

[30] Sobre la viralización de las noticias falsas, puede verse el clásico artículo de VOSOUGHI, S.; ROY, D. & ARAL, S. 2018. The spread of true and false news online. *MIT Initiative on the Digital Economy*.

[31] Se trata de la declaración suscrita en 2017 por el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Relator Especial de la OEA para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) donde manifiestan "*(…) preocupación* por el hecho de que la desinformación y la propaganda a menudo se diseñan e implementan con el propósito de confundir a la población y para injerir en el derecho del público a saber y en el derecho de las personas a buscar y recibir, y también transmitir, información e ideas de toda índole, sin consideración de fronteras, que son derechos alcanzados por las garantías legales internacionales de los derechos a la libertad de expresión y opinión".

[32] SERRA CRISTÓBAL, 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: 31.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

internacional, europeo y nacional[33]. Junto con la desinformación, las tecnologías algorítmicas han sido aprovechadas para propagar mensajes nocivos como discursos de odio o discriminación.

Los mismos algoritmos se utilizan para luchar contra aquellos contenidos perniciosos mediante filtrados basados en palabras clave que, si bien pueden tener cierta efectividad para detectar contenidos xenófobos o discriminadores, no resuelven con acierto el filtrado de bulos. Más bien a la inversa, los algoritmos se muestran ineficaces, censurando contenidos no nocivos (una madre dando de mamar a su bebé, una obra artística que incluye un desnudo, etc.), mientras que en otras ocasiones se permiten contenidos violentos (como el asesinato de un animal o una agresión grabada y difundida por las redes). Realmente, el combate contra las noticias falsas plantea una gran complejidad porque incide en el ejercicio de la libertad de expresión, un derecho fundamental y nuclear en democracia que debe salvaguardarse por lo que cualquier restricción o límite no puede suponer un ejercicio de censura.

En la Unión Europea la lucha contra la desinformación se ha instrumentado a través de diversas iniciativas cuyos hitos fundamentales son el *Código de Buenas prácticas en materia de desinformación* de 2018 con el que la UE apuesta claramente por la vía colaborativa en la que las empresas tecnológicas juegan un papel imprescindible en la lucha contra las noticias falsas[34] y el *Reglamento de Servicios Digitales* de 2022 con el que se advierte que, transcurrido el tiempo, la Unión se ha ido decantando hacia una vía regulatoria que imponga obligaciones exigibles a las plataformas tecnológicas ante las limitaciones del enfoque de *soft law* en la lucha contra la desinformación.

[33] Nos referimos a la consideración de las noticias falsas y la desinformación como integrantes del concepto de amenazas híbridas en el que la transmisión de informaciones falseadas y la manipulación de los medios y redes sociales se emplean con el objetivo de desestabilizar Estados y radicalizar a la sociedad. Sobre la cuestión véase el documento de referencia en España, *Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil* (Presidencia del Gobierno, Departamento de Seguridad Nacional, marzo 2022), que se enmarcó en la estrategia de la Unión Europea para hacer frente a las campañas de desinformación, que se recoge tanto en el *Plan de Acción contra la desinformación*, de diciembre de 2018, como en el *Plan de Acción para la Democracia Europea,* de diciembre de 2020.

[34] En mayo de 2021, la Comisión Europea publicó unas Directrices para el reforzamiento del Código de Buenas Prácticas en materia de Desinformación: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Comittee of the Regions, European Commission *Guidance on Strengthening the Code of Practice on Disinformation,* Brussels, 26.5.2021, COM(2021) 262.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

4.- Transparencia algorítmica: los elementos clave de los algoritmos que determinan la creación y difusión de información

La transparencia algorítmica es una herramienta básica como instrumento de garantía de una serie de principios democráticos y derechos fundamentales. Porque, desde una perspectiva externa, permite a los afectados, interesados o público en general: a) verificar la actuación de programadores que han traducido el código jurídico en código informático; b) cumplir con las obligaciones de transparencia, información y derecho de acceso que impone el régimen de protección de datos; c) controlar errores, discriminación y sesgos algorítmicos; y d) defenderse frente a las decisiones basadas en sistemas algorítmicos. Asimismo, la transparencia interna o técnica es un instrumento esencial para el conocimiento y comprobación del funcionamiento correcto del algoritmo por todos los sujetos implicados en su funcionamiento y su revisión (programadores, analistas, auditores, jueces, etc.).

El ejercicio de transparencia algorítmica puede verse limitado, como vimos, por algunas cuestiones como la propiedad intelectual o la normativa sobre secretos comerciales como límites al derecho de información de los interesados, pero el marco regulatorio de la propiedad intelectual o el secreto comercial no deberían impedir dicha transparencia por parte de las empresas periodísticas o tecnológicas[35]. Los negocios también se han señalado como obstáculo para la transparencia[36], es decir, la falta de incentivos comerciales para la divulgación porque la transparencia implica costes como la preparación de los datos, la redacción de informes, la mejora del código fuente y los testeos de comprobación. Otros obstáculos son la privacidad que puede causar problemas si los datos no están adecuadamente anonimizados, así como las implicaciones legales de admitir errores que podrían conllevar hasta demandas judiciales. Incluso la creación de un ambiente de desconfianza entre la audiencia: si la empresa reconoce que hay un 80% de veracidad en una pieza de información concreta – que puede ser un nivel muy legítimo desde el punto de vista científico – quizá la audiencia deduzca que el artículo periodístico es inválido. Finalmente, se ha hecho referencia a los riesgos comerciales existentes ya que revelar aspectos de cómo funciona el algoritmo puede perjudicar la ventaja competitiva tecnológica de una organización o amenazas para la ciberseguridad derivados de la transparencia de los modelos de aprendizaje automático en tanto

[35] En el marco del RGPD, el GT29 ha indicado que, si bien se prevé cierta protección para los responsables, estos no pueden basarse en la protección de sus derechos comerciales como excusa para denegar el acceso o negarse a ofrecer información al interesado. (GRUPO DE TRABAJO DEL ARTÍCULO 29, *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 el 6 de febrero de 2018, p. 19).

[36] DIAKOPOULOS, N. & KOLISKA, M. 2017. "Algorithmic transparency in the news media". *Digital Journalism*, vol. 5, núm. 7: 821-824.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

que su publicidad supondría abrir el sistema a la manipulación por parte de terceros y ello repercutiría a su vez en la eficiencia del algoritmo.

Frente a estas desventajas, la confianza, la credibilidad, la reputación y la legitimación son los principales factores que deben destacarse como resultados positivos de la transparencia algorítmica.

Por tanto y descendiendo a un nivel más concreto, la principal cuestión a resolver es qué elementos debemos conocer esencialmente sobre los algoritmos que determinan la creación y difusión de información.

El principal elemento que debe tenerse en cuenta es la *implicación humana* en los algoritmos porque es básica para su diseño y funcionamiento. Así, es interesante conocer las influencias humanas editoriales, las decisiones en la modelación y metodología y la manera como esas opciones editoriales se implementan en el código del algoritmo. Debe suministrarse información sobre esas decisiones editoriales en el proceso de diseño del algoritmo porque permiten ver qué noticias se dejan fuera y aclaran la línea editorial de la organización. Piénsese en la importancia de que la pluralidad y la diversidad como valores periodísticos estén integrados en el diseño del algoritmo frente a otros valores como los económicos.

En el caso de la generación automática de noticias, debe etiquetarse si un editor humano ha revisado el *output* antes de la publicación porque es determinante para la credibilidad del resultado.

También ha de conocerse la identidad de las personas que tienen control sobre el sistema algorítmico o son responsables. Los diseñadores de estos sistemas deben hacerse públicos de forma similar a la declaración de autoría de los artículos. En algunos casos, las entidades compran el *software* en lugar de crearlo, lo que supone que la involucración de la persona no está en el diseño del código del algoritmo sino en su parametrización y configuración.

En segundo lugar, los *datos* configuran otro elemento esencial de los sistemas algorítmicos y es necesario conocer cómo se seleccionan. Los algoritmos tienen una dependencia innegable de los datos que permiten el funcionamiento del aprendizaje autónomo, la personalización, simulación y escritura automatizada de historias. Las dimensiones clave que deben hacerse públicas son la calidad y validez de los datos que alimentan el sistema. Concretamente, esto incluye variables como la precisión de los datos, seguridad (p. ej. márgenes de error), actualidad (p. ej. cuándo se recopilaron los datos), exhaustividad o complitud, método de muestreo, procedencia (por ejemplo, fuentes públicas o privadas de las que proceden los datos o si incluyen información personal) y volumen (por ejemplo, de los datos de entrenamiento utilizados en el aprendizaje automático).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

En tercer lugar, el modelo o *programación del algoritmo* que realiza las inferencias a partir de los datos de entrada, esto es, qué rasgos o variables emplea el algoritmo y su parametrización. Se tiene que saber qué optimiza el algoritmo, cómo equilibra rasgos e infiere resultados para hacer clasificaciones de los contenidos o recomendaciones. Sobre el alcance de la información, se apuesta por la publicidad del código fuente aunque existen dudas sobre la utilidad para el gran público de conocer esa información por tratarse de información muy técnica.

Por último, la transparencia también debe aplicarse a la parte final del proceso que es la que *interactúa con los usuarios.* Cualquier información sobre el algoritmo tiene que ofrecerse de forma visual. En su versión más sencilla, la "presencia del algoritmo" puede indicarse con un icono en la interfaz junto al contenido que se ha producido por un sistema algorítmico, como el contenido personalizado.

5.- La transparencia algorítmica en la producción de la UE y su aplicación a los medios de comunicación y plataformas tecnológicas

Los avances regulatorios en la UE para impedir el desconocimiento de los riesgos y posibles efectos dañinos de esta actividad algorítmica han sido especialmente intensos en los últimos años. El objetivo de la Unión es conseguir que el espacio digital se construya como un entorno seguro y que el marco de derechos humanos se convierta en un componente fundamental del ámbito de la ética de los datos, del uso de los algoritmos y de la inteligencia artificial.

En un análisis forzosamente breve de este marco regulatorio[37], nos centramos en aquellas disposiciones que se refieren a la transparencia algorítmica y su alcance, contenido y consecuencias en el contexto de los medios y plataformas digitales.

[37] Según recuerda Cotino, el principio de transparencia algorítmica es el principio de referencia de la inteligencia artificial confiable y lo ejemplifica con diversos estudios que lo localizan en más de 84 documentos políticos sobre IA o en el 94% de los documentos analizados sobre los principios éticos de la IA (COTINO HUESO, L. 2022. "Transparencia y explicabilidad de la inteligencia artificial y "compañía…", *cit.,* pp. 28 y 29). Por su relevancia, mencionamos la reciente *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*, de 26 de enero de 2023, en cuyo capítulo III sobre Libertad de elección dedica un apartado a las "Interacciones con algoritmos y sistemas de inteligencia artificial" y declara el compromiso de "b) velar por un nivel adecuado de transparencia en el uso de los algoritmos y la inteligencia artificial y por que las personas estén informadas y capacitadas para utilizarlos cuando interactúen con ellos" así como el Reglamento europeo en materia de terrorismo que contempla la adopción de "medidas proactivas" de los proveedores de servicio para proteger frente a la difusión de contenidos terroristas y toda una serie de garantías frente a la posible afectación a derechos y libertades fundamentales de estas medidas como son las obligaciones de transparencia, de información y de motivación de las decisiones (arts. 7 y 8) (Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo de 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea, DOUE 17.5.2021)

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

La primera referencia a esta obligación la encontramos en el *RGPD* que es la norma que determina las características sobre las que se construye el régimen europeo de protección de datos entre las que destacan algunos principios con especial proyección en el tratamiento de datos masivos por algoritmos como el principio de legitimación del tratamiento, el principio de calidad de los datos o el principio de transparencia consagrado en el artículo 22.1 que establece la prohibición general de tomar decisiones automatizadas, incluida la elaboración de perfiles, que tenga efectos jurídicos sobre el interesado o le afecte significativamente aunque el precepto contempla algunas excepciones muy matizadas.

Según el GT29[38], la decisión a que se refiere el artículo 22 RGPD debe afectar a los derechos o al estatuto jurídico de la persona que se ve sometida a ese específico tratamiento (p. ej. la cancelación de un contrato o la denegación automática de la ciudadanía). Con respecto a las decisiones que puedan afectar significativamente de modo similar, resulta más difícil precisar lo que se considera "suficientemente equitativo" lo que ha provocado distintas interpretaciones doctrinales[39] aunque interesa destacar que "el derecho individual a una explicación puede no proteger frente a efectos jurídicos generales, como, por ejemplo la publicidad personalizada o las noticias falsas"[40], prácticas que impactan de modo colectivo en la sociedad con una capacidad de afectación a bienes colectivos[41].

Asimismo, el apartado 3 del mencionado artículo 22 RGPD exige que los responsables adopten las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de los interesados, como mínimo, el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión, Aunque exista controversia respecto del derecho a una explicación sobre la concreta

[38] GRUPO DE TRABAJO DEL ARTÍCULO 29, Directrices sobre decisiones individuales automatizadas y elaboración de perfiles…, cit.

[39] Un análisis de las interpretaciones restrictivas y amplias del alcance del artículo 22 RGPD puede verse en ROIG, A. 2020. *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Bosch. Barcelona, especialmente, pp. 70 y 92-95.

[40] ROIG, A. *cit.* p. 74.

[41] De ahí que se propugne un enfoque sobre el desarrollo algorítmico que supere la dimensión individual y tenga en cuenta los perjuicios que genera en los derechos fundamentales de sectores o conjuntos de la sociedad (por todos, AÑÓN ROIG, M. J. 2022. "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos". *Derechos y libertades*, núm. 47: 47 y COTINO HUESO, L. 2017. "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata*, año 9, núm. 24: 137).

CC BY SA

DOI: https://doi.org/10.51915/ret.308

decisión tomada por el algoritmo[42], el RGPD ha configurado un régimen reforzado de transparencia algorítmica que reconoce al interesado el derecho a estar informado por los responsables sobre cómo y para qué se utiliza su información, incluida la lógica utilizada en los algoritmos para determinar las suposiciones y predicciones sobre él[43].

La siguiente referencia es la *propuesta de Reglamento de Inteligencia Artificial*[44] con la que la UE ha definido las piedras angulares del enfoque europeo de la IA para los años venideros y que termina de superar la fase de primera lectura con aprobación de enmiendas en el Parlamento Europeo[45]. Pretende un doble objetivo, a saber, por una parte, la creación de un mercado único digital europeo que sea competitivo, favorable a la innovación y no dominado por el reducido grupo de multinacionales tecnológicas no europeas y, por otra, fomentar la seguridad jurídica y garantizar que los europeos puedan aprovechar nuevas tecnologías que se desarrollen y funcionen de acuerdo con los valores europeos, consagrados en la Carta Europea de Derechos Fundamentales, el Convenio Europeo de Derechos Humanos, y también el Directrices europeas de ética de la IA.

En cuanto a su naturaleza, el futuro Reglamento es una norma directamente aplicable en los 27 Estados miembros con lo que se trata de lograr un efecto homogeneizador tan relevante en este ámbito de utilización de las tecnologías. Además, al igual que ocurre con el RGPD, la propuesta de Reglamento tiene un efecto extraterritorial porque sus obligaciones también pueden aplicarse a proveedores y usuarios profesionales de los sistemas de IA establecidos en un tercer país, siempre que sus sistemas estén comercializados, situados o utilizados en la UE. Concretamente, esto significa que los proveedores de, por ejemplo, sistemas

[42] Puede verse un claro resumen del debate en RODRÍGUEZ MARTÍNEZ, G. 2020. "La transparencia algorítmica en el tratamiento de los datos personales". *Revista de Privacidad y Derecho Digital*, núm. 17: 61-92.

[43] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, Opinion 7/2015 "Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability", 19 de noviembre de 2015.

[44] 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, Bruselas, 21.4.2021, COM (2021) 206 final. El 14 de junio de 2023, los eurodiputados adoptaron su posición negociadora sobre el Reglamento de IA que dio inicio a las conversaciones sobre la forma final del Reglamento en el Consejo, junto a los países de la UE.

[45] Enmiendas adoptadas por el Parlamento Europeo el 14 de junio de 2023 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. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

algorítmicos de moderación y recomendación de contenidos que se encuentran fuera de la UE y ofrezcan sus productos a organizaciones de medios dentro de la UE tendrán que observar los requisitos del Reglamento de IA. Lo mismo ocurrirá con un sitio web de noticias fuera de la UE que interactúe con los consumidores en la UE, p. e. través de un chatbot o producción de contenido automatizado dirigido a usuarios concretos.

Un elemento central de la propuesta de Reglamento de IA es distinguir entre *aplicaciones inaceptables de IA* (por ejemplo, calificación de riesgo social y manipulación subliminal), *IA de alto riesgo***,** que son riesgos manejables que pueden abordarse a través de la transparencia y las aplicaciones de *bajo riesgo* para las cuales promueve la autorregulación.

En principio, los sistemas de IA utilizados en periodismo no encajan en la IA de alto riesgo aunque planteamos que el impacto de las plataformas algorítmicamente impulsadas en el ejercicio de derechos como la libertad de expresión y el derecho a la intimidad aconsejarían etiquetar los algoritmos utilizados en la categoría de alto riesgo. El poder de estas plataformas para habilitar o restringir la libertad global de expresión es innegable. El propio Tribunal Europeo de Derechos Humanos ha confirmado "la importancia de los sitios de internet para el ejercicio de la libertad de expresión"[46] puesto que internet "se ha convertido en una de las principales vías a través de las cuales los individuos ejercen su derecho a la libertad de expresión e información"[47].

La obligación más relevante en la propuesta de Reglamento de IA para los medios consiste en informar a los usuarios si están interactuando con un sistema de inteligencia artificial, salvo que sea evidente por las circunstancias y el contexto de uso (artículo 52.1 de la Propuesta). Este deber de notificación significa que si una organización de medios utiliza un *chatbot*, un agente virtual, un sistema de optimización para la distribución de noticias, un sistema automatizado de escritura o un recomendador de noticias para interactuar con las audiencias, ese sistema tendría que ser diseñado de una manera para informar a la audiencia sobre el hecho de que es una IA, no un ser humano, con quien interactúan.

Con cierto realismo, debemos cuestionarnos si las obligaciones de transparencia son realmente suficientes para abordar los riesgos para los intereses de los consumidores y para los derechos fundamentales. La pura notificación a los usuarios de que una selección del contenido de noticias se recomienda a través de un sistema de inteligencia artificial, en lugar de un editor humano, dice en sí mismo muy poco sobre la calidad de la recomendación y si el sistema ha sido diseñado teniendo

[46] STEDH de 1 de diciembre de 2015, asunto *Cengiz y otros c. Turquía*, par. 52.

[47] STEDH de 18 de diciembre 2012, asunto *Ahmet Yıldırım c. Turquía*, par. 54.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

presentes los valores editoriales profesionales, el grado con el que se han verificado los resultados de la IA en busca de sesgos, si priorizan los intereses de los usuarios, si son imparciales o están protegidos contra la piratería informática y otras formas de ataques maliciosos o manipulación[48].

También resultan preocupantes las manipulaciones a las que se refiere el artículo 52.3 de la Propuesta de Reglamento de IA que estipula que los usuarios de sistemas de generación de medios sintéticos deben divulgar el hecho de que el contenido haya sido generado o manipulado artificialmente. Se trata de las polémicas ultrafalsificaciones o *deepfakes* que permiten a los medios generar archivos manipulados mediante un software de inteligencia artificial programados para producir imágenes, videos, voz o texto que reflejen la personalidad o el estilo de los datos con que fueron entrenados. La generación de voz sintética para imitar la voz de una periodista en un podcast o en una versión leída de cualquier artículo; el uso de esta tecnología para producir un vídeo de un presentador de noticias para leer los titulares del día serían ejemplos que obligan a los editores de medios a etiquetar dicho uso lo que puede ayudar a los usuarios a comprender cualquier discrepancia o inexactitud introducida por el sistema de IA.

Finalmente, analizamos las referencias a la transparencia algorítmica contenidas en el *Reglamento de Servicios Digitales*[49]. La proliferación de la desinformación, la exclusión digital, la interferencia extranjera en procesos democráticos y la polarización en la sociedad son consecuencias muy negativas del espacio digital y, en este sentido, también el Reglamento de Servicios Digitales reconoce que el uso de sistemas automatizados de moderación y recomendación de contenidos puede ser la fuente de riesgos sistémicos para los derechos fundamentales que son lo suficientemente graves como para justificar regulación, al menos cuando está en manos de plataformas en línea de muy gran tamaño. Por ello, la normativa se inscribe en la línea de articular responsabilidades claras a las plataformas y regular los

[48] Este mismo cuestionamiento en HELBERGER, N. & DIAKOPOULOS, N. 2022. "The European AI Act and How It Matters for Research into AI in Media and Journalism". *Digital Journalism*, p. 4.

[49] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

CC BY SA

DOI: https://doi.org/10.51915/ret.308

algoritmos de recomendación en Internet y la denuncia de contenidos dañinos o que promuevan la desinformación[50].

Efectivamente, esta norma coloca la desinformación en el centro del debate y explica que la manipulación informativa amenaza la democracia por lo que promueve tomar medidas ante la capacidad de "generar información deliberadamente incorrecta o engañosa" (Considerando 104) y se propone actuar contra "las cuentas falsas, el uso de bots y (…) comportamientos total o parcialmente automatizados, que pueden dar lugar a la difusión rápida y extendida de información que sea un contenido ilícito o incompatible con las condiciones generales de una plataforma en línea o un motor de búsqueda en línea y que contribuya a campañas de desinformación" (Considerando 84). Por ello, establece mecanismos de eliminación de contenidos ilícitos y de protección de los derechos fundamentales de los usuarios, incluida la libertad de expresión. Además, el Reglamento de Servicios Digitales introduce una mayor supervisión pública de las plataformas, en particular, las grandes tecnológicas, con una media de usuarios activos mensuales igual o superior a 45 millones (más del 10 % de la población de la UE).

Asimismo, y en línea con lo que establece la propuesta de Reglamento sobre IA, obliga a los prestadores de servicios a suministrar información sobre cualesquiera políticas, procedimientos, medidas y herramientas empleadas para moderar los contenidos, incluidas la toma de decisiones mediante algoritmos y la revisión humana (artículo 14) lo que permitirá conocer los elementos que condicionan que unos contenidos aparezcan más arriba o abajo en las búsquedas o en los mensajes de las redes sociales. Las plataformas deben presentar con claridad los parámetros de dichos sistemas de recomendación de manera fácilmente comprensible con el fin de asegurarse de que los destinatarios del servicio entienden cómo se prioriza la información para ellos.

Finalmente, el Reglamento contiene la prohibición de determinado tipo de anuncios selectivos en las plataformas en línea cuando están dirigidos a menores o cuando utilizan categorías especiales de datos personales, como la etnia, las opiniones políticas o la orientación sexual. En el resto de casos de publicidad en línea, las

[50] Aunque no sea objeto de este análisis, debe señalarse que se ha producido una evolución en la jurisprudencia del Tribunal de Justicia de la UE respecto a la obligatoriedad de sistemas automatizados de control de contenidos por parte de las plataformas en la que, hasta tiempos recientes, se ha mantenido en la interpretación de la prohibición de que se impusieran sistemas de filtrado activo de los contenidos difundidos a través de las plataformas sobre la base de que este tipo de medidas resultaban desproporcionadas tanto a nivel tecnológico como por su impacto en la libertad de expresión. Sobre esta cuestión, por todos, TERUEL LOZANO, G. M. 2023. "Libertad de expresión, censura y pluralismo en las redes sociales: algoritmos y el nuevo paradigma regulatorio europeo". *Derecho Público de la Inteligencia Artificial*. F. Balaguer Callejón y L. Cotino Hueso (coords.). Fundación Giménez Abad, pp. 196-204.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

plataformas están obligadas a prestar información individualizada a los destinatarios que les sea necesaria para saber cuándo y en nombre de quién se presenta el anuncio así como los parámetros utilizados para determinar que se les presente un anuncio determinado[51].

Lo cierto es que la opción autorregulatoria basada en la voluntariedad de las empresas tecnológicas de acogerse a códigos de conducta no ha dado resultados satisfactorios y, a día de hoy, se les debe considerar como los nuevos mediadores de los procesos comunicativos. Ocupan una posición de cuasi-monopolio y se ha comprobado que contribuyen a la percepción de lo que se considera la verdad en el espacio público por lo que, con las cautelas apropiadas, el enfoque del Reglamento de Servicios Digitales es oportuno para proteger la esfera política y social de la acción de las plataformas que, mediante sus algoritmos, promueven una narrativa deformada que les proporciona mayores réditos económicos pero que ponen en riesgo el debate público esencial en democracia al que nos referíamos al inicio de estas líneas.

6.- Conclusiones

La transparencia se ha convertido en un valor central en las sociedades actuales respaldado por su consideración como derecho de la ciudadanía en numerosos textos normativos que inciden cada vez en más ámbitos (decisiones públicas, publicidad electoral, etc.) y por una correlativa demanda de transparencia en la sociedad a lo largo del tiempo.

Esta demanda de transparencia ha alcanzado a los medios de comunicación y a las plataformas digitales proyectándose sobre los algoritmos como herramientas clave en sus negocios completamente adaptados al entorno digital.

En las redacciones digitales se emplean los potentes y complejos algoritmos de IA para todo el proceso periodístico: desde la recogida y selección automatizada de información hasta la relación con la audiencia, pasando por la producción de noticias y su distribución. Por su parte, toda la actividad de las plataformas de redes sociales descansa en el tratamiento algorítmico de volúmenes masivos de datos que conocen de sus usuarios y terceros.

A pesar de que las características de los algoritmos plantean dificultades para su conocimiento público (como derechos que protegen la propiedad intelectual o el

[51] En el marco del Reglamento de Servicios Digitales, el Centro Europeo de Transparencia Algorítmica de la Unión Europea, cuya sede se ha ubicado recientemente en Sevilla, se encargará de la realización de análisis técnicos y evaluaciones de algoritmos, basándose en informes de transparencia y autoevaluación de riesgos de las empresas designadas; la propuesta de buenas prácticas que atenúen sus repercusiones negativas; así como la investigación de los efectos sociales a largo plazo de los algoritmos.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia algorítmica en los medios…
por Cristina Pauner Chulvi
Págs. 107-136
DOI: https://doi.org/10.51915/ret.308

secreto comercial), debe poder comprobarse su diseño, funcionamiento y resultados porque está demostrado que los sesgos, los errores de configuración o la inexactitud de los datos producen impacto en derechos fundamentales de los individuos, derechos como la protección de datos, la libertad de información o la no discriminación.

Por eso, la Unión Europea, seguida por muchos países, han consagrado la transparencia normativa en numerosos textos jurídicos en los que se configura desde una doble perspectiva: interna o técnica, esencial para el conocimiento y comprobación del funcionamiento del sistema por quienes participan en el funcionamiento, explotación o revisión del mismo y externa o general, como garantía de principios y derechos constitucionales.

El estudio de la propuesta de Reglamento de IA y del Reglamento de Servicios Digitales ha mostrado un elenco de medidas para mitigar los riesgos de la manipulación informativa y garantizar los derechos de los usuarios a quienes habrá que advertir si están interactuando con un sistema de inteligencia artificial, incluidas las ultrafalsificaciones; informar a los destinatarios sobre los parámetros utilizados para el envío de publicidad en línea, para ordenar la información mostrada a cada persona, etc.

En el caso del periodismo digital, la transparencia algorítmica actuará en beneficio de la percepción del público de la credibilidad, legitimidad y confianza en los medios de comunicación. En el caso de las redes sociales, aunque una transparencia impuesta jurídicamente no es una fórmula mágica que resolverá todos los problemas, sí es un corolario natural del poder que las plataformas tienen sobre nuestro sistema de información.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

Bibliografía

AEPD. 2020. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*.

ALBERTOS, J. L. M. 1994. "La tesis del perro-guardián: revisión de una teoría clásica". *Estudios sobre el mensaje periodístico,* núm. 1: 13-25.

AÑÓN ROIG, M. J. 2022. "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos". *Derechos y libertades*, núm. 47: 17-49.

BLUMLER, J. G. 2018. "The Crisis of Public Communication, 1995-2017". *Javnost-The Public*, vol. 25, núm. 1-2: 83-92.

CAREY, J. 1996. Where journalism education went wrong. *Presentation at the Middle Tennessee State University.*

CARLSON, M. 2014. "The robotic reporter: automated journalism and the redefinition of labor, compositional forms and journalistic authority". *Digital Journalism,* vol. 3(3): 416-431.

CASERO-RIPOLLÉS, A. 2014. "La pérdida de valor de la información periodística: causas y consecuencias". *Anuario ThinkEPI*, núm. 8: 256-259.

COTINO HUESO, L.

- 2022. "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta", en *Transparencia y explicabilidad de la Inteligencia Artificial.* Tirant lo Blanch: Valencia, pp. 25-69.

- 2017. "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata*, año 9, núm. 24: 131-150.

DE LA CUEVA, J. 2018. "Código fuente, algoritmos y fuentes del Derecho". *Notario del siglo XXI,* núm. 77, disponible en https://www.elnotario.es/index.php/opinion/8382-codigo-fuente-algoritmos-y-fuentes-del-derecho.

DIAKOPOULOS, N. & KOLISKA, M. 2017. "Algorithmic transparency in the news media". *Digital Journalism*, vol. 5, núm. 7: 809-828. DOI: 10.1080/21670811.2016.1208053

ELÍAS, C. 2015. *Big data y periodismo en la sociedad red*. Editorial Síntesis: Madrid.

CC BY SA

FLORES-VIVAR, J. M. 2018. «Algoritmos, aplicaciones y Big data, nuevos paradigmas en el proceso de comunicación y de enseñanza-aprendizaje del periodismo de datos». *Revista de Comunicación*, vol. 17, núm. 2: 268-291.

GARCÍA-GORDILLO, M. M.; PALAU-SAMPIO, D. y RIVAS-DE-ROCA, R. 2022. "Pero ¿qué me cuentas? Una revisión del concepto de verdad en el siglo XXI", en Caro-González, F. J.; Garrido-Lora, M.; García-Gordillo, M. M. (eds.), *El problema de la verdad. Retos y riesgos en la comunicación*. Comunicación Social Ediciones y Publicaciones: Salamanca, pp. 61-81.

GRUPO DE TRABAJO DEL ARTÍCULO 29, *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 el 6 de febrero de 2018.

HELBERGER, N. & DIAKOPOULOS, N. 2022. "The European AI Act and How It Matters for Research into AI in Media and Journalism". *Digital Journalism*. DOI: 10.1080/21670811.2022.2082505

KOVACH, B. & ROSENSTIEL, T. 2001. *The elements of journalism. What news people should know and the public should expect*. Three Rivers Press: New York.

KOLISKA, M. 2022. "Trust and journalistic transparency online". *Journalism Studies*, vol. 23, núm. 12: 1488-1509. DOI: 10.1080/1461670X.2022.2102532.

LATAR, N. L. 2015. "The Robotic Journalist in The Age of Social Physics: The End of Human Journalism?", in G. Einav (ed.), *The New World of Transition Media*. Springer International Publishing: Swiss, pp. 65-80.

MAGALLÓN ROSA, R. 2021. "Medios de comunicación y redes sociales: entre el conflicto, la (in)dependencia y la colaboración". *Cuadernos de Periodistas*, núm. 42: 9-17.

MANFREDI SÁNCHEZ, J. L. y UFARTE RUÍZ, M. M. 2020. "Inteligencia artificial y periodismo: una herramienta contra la desinformación*. *Revista CIDOB d'Afers Internacionals*, núm. 124: 49-72.

MARTÍNEZ-COSTA, M. P. 2018. "El mercado de los medios digitales en España". *Cuadernos de Periodistas*, núm. 37: 77-84.

MARTÍNEZ MARTÍNEZ, R. "Team Jorge: Desinformación, derechos fundamentales y democracia". *Agenda Pública*, 28 de febrero de 2023.

MÉNDEZ, L. 2021. "El algoritmo sustituye al periodismo". *Cuadernos de Periodistas*, núm. 42: 65-70.

MEYER, P. 1975. "Precision journalism". *Communication Information*, vol. 1, núm. 1: 164-165.

CC BY SA

DOI: https://doi.org/10.51915/ret.308

OWEN, D. 2018. "El papel de los nuevos medios en la política", en *La era de la perplejidad. Repensar el mundo que conocíamos*. Taurus: Barcelona.

PARISER, E. 2011. *The filter buble. What the Internet is hiding from you*. Penguin Press. London.

PAUNER CHULVI, C. 2022. "Sobre la compleja relación entre los medios de comunicación y las plataformas tecnológicas: Google News y los derechos de autor", *Revista de Derecho Político*, núm. 115: 43-72.

RODRÍGUEZ MARTÍNEZ, G. 2020. "La transparencia algorítmica en el tratamiento de los datos personales". *Revista de Privacidad y Derecho Digital*, núm. 17: 61-92.

ROIG, A. 2020. *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Bosch. Barcelona.

SALAVERRÍA, R.

- 2019. "Digital journalism: 25 years of research. Review article". *El profesional de la información*, vol. 28, núm. 1. https://doi.org/10.3145/epi.2019.ene.01.

- 2014. "Periodismo en 2014: balance y tendencia". *Cuaderno de Periodistas*, núm. 29: 9-22.

SALAZAR, I. 2018. "Los robots y la Inteligencia Artificial. Nuevos retos del periodismo", *Doxa Comunicación,* núm. 27: 295-315.

SÁNCHEZ-GARCÍA, P.; MERAVO-ÁLVAREZ, N.; CALVO-BARBERO, C. & DIEZ-GRACIA, A. 2023. "Desarrollo tecnológico español de la inteligencia artificial aplicada al periodismo: empresas y herramientas de documentación, producción y distribución de información". *Profesional de la Información*, vol, 32, núm. 2.

SERRA CRISTÓBAL, 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: 13-46.

STRÖMBACK, J. 2005. "In Search of a Standard: four models of democracy and their normative implications for journalism". *Journalism Studies*, vol. 6:3: 331-345, DOI: 10.1080/14616700500131950

SUNSTEIN, C. R. 1999. "The Law of Group Polarization". John M. Olin Program in *Law & Economics Working Paper*, núm. 91.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, *Opinion 7/2015 "Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability"*, 19 de noviembre de 2015.

CC BY SA

TERUEL LOZANO, G. M. 2023. "Libertad de expresión, censura y pluralismo en las redes sociales: algoritmos y el nuevo paradigma regulatorio europeo". *Derecho Público de la Inteligencia Artificial*. F. Balaguer Callejón y L. Cotino Hueso (coords.). Fundación Giménez Abad.

TÚÑEZ-LÓPEZ, M.; TOURAL-BRAN, C. y VALDIVIEZO-ABAD, C.

- 2019. "Automatización, bots y algoritmos en la redacción de noticias. Impacto y calidad del periodismo artificial". *Revista Latina de Comunicación Social*, núm. 74: 1411-1433.

- 2018. "Uso de bots y algoritmos para automatizar la redacción de noticias: percepción y actitudes de los periodistas en España". *El Profesional de la Información*, vol. 27, núm. 4: 1699-2407.

VAN DALEN, A. 2012. "The algorithms behind the headlines". *Journalism Practice*, vol. 6, issue 5-6: 648-658, DOI: 10.1080/17512786.2012.667268.

VENTURA POCINO, P. 2021. *Algoritmos en las redacciones: Retos y recomendaciones para dotar a la inteligencia artificial de los valores éticos del periodismo*. Consell de la Informació de Catalunya.

VILLAVERDE MENÉNDEZ, I. 2004. *Estado democrático e información: el derecho a ser informado*, Junta General del Principado de Asturias: Oviedo.

VOSOUGHI, S.; ROY, D. & ARAL, S. 2018. The spread of true and false news online. *MIT Initiative on the Digital Economy*.

WÖLKER, A. & POWELL, T. E. 2018. "Algorithms in the newsroom? News readers'perceived credibility and selection of automated journalism". *Journalism*, vol. 22, issue 1: 86-103, https://doi.org/10.1177/1464884918757072

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las exigencias de transparencia para los sistemas algorítmicos…
por Ana Garriga Domínguez
Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales

Ana Garriga Domínguez[1]

Universidad de Vigo
España

ORCID: 0000-0003-2846-3448

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

Este trabajo se ha realizado en el marco del proyecto de investigación DATATRANSCO con referencia n.º PID2021-128309NB-I00.

RESUMEN: En este trabajo se recogen las principales problemáticas que suscitan los sistemas de inteligencia artificial, que determinados prestadores de servicios en Internet emplean para personalizar la publicidad en línea y para seleccionar y recomendar información y contenidos. Se estudian las obligaciones derivadas del Reglamento General de Protección de Datos, con particular atención al principio de responsabilidad proactiva y transparencia, en relación con esos sistemas. Finalmente, se abordan las novedades que, en materia de transparencia, introduce el nuevo Reglamento Europeo de Servicios Digitales. Particularmente se estudian las nuevas obligaciones de transparencia algorítmica y rendición de cuentas para los motores de búsqueda en línea de muy gran tamaño y las plataformas en línea de muy gran tamaño, considerando que el nuevo Reglamento ofrece herramientas muy útiles y garantías importantes para luchar contra la desinformación y proteger el derecho a recibir informaciones plurales, la libertad de expresión e ideológica, así como para prevenir la difusión de contenido ilícito o dañino.

[1] Profesora Titular de Filosofía del Derecho y, desde 2019, Delegada de Protección de Datos de la Universidad de Vigo. Su labor docente mayoritaria la realiza en la Escuela Superior de Ingeniería Informática de esta Universidad, de la que ha sido Directora. Es, asimismo, Directora del Laboratorio "Sociedad de la Información y derechos humanos" de la Universidad de Vigo (Laboratorio Consolider-Ingenio 2010 "El tiempo de los derechos"). Ha sido Investigadora principal en numerosos Proyectos de investigación y colaboradora con instituciones públicas y privadas en actividades de I+D y es autora de numerosas publicaciones sobre derechos fundamentales, sociedad de la información y protección de datos personales.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las exigencias de transparencia para los sistemas algorítmicos…
por Ana Garriga Domínguez
Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

PALABRAS CLAVE: Inteligencia artificial, sistemas de recomendación, transparencia algorítmica, protección de datos personales, desinformación.

CONTENIDOS: 1.-Sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea. Riesgos para los derechos fundamentales. 2.-Las garantías derivadas del principio de transparencia en el Reglamento General de Protección de Datos. *2.1.-Decisiones automatizadas y elaboración de perfiles. 2.2.-La importancia de los principios de transparencia y de responsabilidad proactiva del RGPD*[2] *en los sistemas de IA.* 3.-Obligaciones específicas para VLOP y VLOSE en el Reglamento (UE) 2022/2065, de 19 de octubre, de Servicios Digitales (RSD). Especial referencia a las obligaciones de transparencia algorítmica. *3.1.- Un Reglamento para crear un entorno en línea seguro y frenar la difusión de desinformación y manipulación en línea. 3.2.- Obligaciones de transparencia para los motores de búsqueda (VLOSE) y las plataformas en línea de muy gran tamaño (VLOP). Especial referencia a las obligaciones de transparencia algorítmica.* 4.-Conclusión.

Transparency requirements for algorithmic recommender systems, content selection and online advertising in the new European Digital Services Act

ABSTRACT: This paper addresses the main issues raised by artificial intelligence systems, which are used by certain Internet service providers to personalise online advertising and to select and recommend information and content. It examines the obligations arising from the General Data Protection Regulation (GDPR), with particular attention to the principle of proactive liability and transparency, in relation to these systems. Finally, it deals with the new developments introduced by the new European Digital Services Act (DSA) in the field of transparency. In particular, the new algorithmic transparency and accountability obligations for very large online search engines and very large online platforms are studied, considering that the new Regulation offers useful tools and important guarantees to fight disinformation and protect the right to receive pluralistic information, freedom of expression and ideology, as well as to prevent the dissemination of illegal or harmful content.

KEYWORDS: Artificial intelligence, recommender systems, algorithmic transparency, personal data protection, disinformation.

[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).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

1.- Sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea. Riesgos para los derechos fundamentales

En los últimos años se ha producido un espectacular desarrollo tecnológico, que ha tenido como protagonista el avance en los sistemas de Inteligencia Artificial (IA). Su desarrollo es comparable al que, en las dos décadas anteriores, experimentó Internet y con el vertiginoso incremento del número y clase de servicios disponibles a través de la red usados por millones de personas. Su evolución, desde la IA simbólica, que se basaba en reglas predefinidas ejecutadas por una máquina, a la IA que se sirve de grandes conjuntos de datos (Big Data) y que se basa en el aprendizaje automático, ha tenido como consecuencia el incremento de su número de aplicaciones y de su capacidad para resolver problemas. Pero, su desarrollo y aplicación no ha estado exenta de críticas y cuestionamientos por los problemas que muchos de estos sistemas plantean por su injerencia en los derechos fundamentales y los valores democráticos. Un ejemplo muy reciente lo tenemos en el sistema de IA generativa, *ChatGPT*[3]*,* que permite a cualquier usuario mantener conversaciones, producir textos sobre temáticas diversas, facilitar respuestas planteadas por los usuarios (en ocasiones exactas, en otras con errores e inexactitudes) y que tiene un sentido del contexto que le permite mantener una conversación con su interlocutor coherente con su interacción con ella. Se trata de un sistema que puede realizar multitud de tareas, desde escribir líneas de código a redacciones o poemas y, por supuesto, mantener una conversación sobre cualquier temática. Desde su lanzamiento en abierto, hemos pasado del asombro y la expectación a la preocupación por sus efectos, en el ámbito educativo, respecto de los derechos de propiedad intelectual, por los riesgos éticos en muchos ámbitos y por su capacidad para difundir desinformación, hasta el punto de que más de un millar de expertos en IA han pedido una moratoria de seis meses[4] para "la carrera sin control de los *ChatGPT*"[5]. Y si bien, esa petición se ha cuestionado por determinados séctores[6], lo

[3] Según se describe por su desarrollador, OpenAI, ChatGPT es un modelo lingüístico diseñado para responder a consultas basadas en texto y generar respuestas en lenguaje natural. Forma parte del campo más amplio de la inteligencia artificial conocido como procesamiento del lenguaje natural (PLN), que trata de enseñar a los ordenadores a entender e interpretar el lenguaje humano.

ChatGPT se basa en una arquitectura de aprendizaje profundo denominada Transformer, que le permite aprender patrones lingüísticos y generar textos coherentes y similares a los humanos. Puede consultarse en su web: GPT Chatbot: Advanced AI Chat.

[4] El texto de la *carta* puede consultarse en: https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

[5] Véase el reportaje publicado en el diario El País (elpais.com) el 29 de marzo de 2023 bajo el título "Expertos en inteligencia artificial reclaman frenar seis meses la "carrera sin control" de los ChatGPTid.

[6] Véase reportaje publicado en el diario La Opinión (laopinioncoruna.es) "Así responden los expertos de A Coruña a la carta de Elon Musk sobre Inteligencia Artificial y ChatGPT" publicado el 9 de abril de 2023.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las exigencias de transparencia para los sistemas algorítmicos…
por Ana Garriga Domínguez
Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

cierto es que el pasado 30 de marzo, el *Garante per la Proteziones dei Dati Personali* ordenó la medida de limitación provisional del tratamiento de los datos personales de los interesados establecidos en territorio italiano, al entender que se podían estar produciendo varias infracciones graves tipificadas en el RGPD. También la Agencia Española de Protección de Datos (AEPD) ha iniciado una investigación de oficio a OpenAI, propietaria de ChatGPT[7].

Habida cuenta de la existencia de diferentes definiciones de IA, en este trabajo se proponen dos complementarias. Una más amplia, que es la recogida en la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO de noviembre de 2021, según la cual, "los sistemas de IA son tecnologías de procesamiento de la información que integran modelos y algoritmos que producen una capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como la predicción y la adopción de decisiones en entornos materiales y virtuales"; y, otra más estricta y más alineada con la propuesta de la OCEDE, que es la recogida en la última versión de la Propuesta de Reglamento sobre IA[8]. Ésta última, define un sistema de inteligencia artificial como aquel sistema "concebido para funcionar con elementos de autonomía que, a partir de datos e información generados por máquinas o por seres humanos, infiere la manera de alcanzar una serie de objetivos, utilizando para ello estrategias de aprendizaje automático o estrategias basadas en la lógica y el conocimiento, y produce información de salida generada por el sistema, como contenidos (sistemas de inteligencia artificial generativa), predicciones, recomendaciones o decisiones, que influyen en los entornos con los que interactúa el sistema de IA".

La IA tienen múltiples aplicaciones y en muchas de ellas se emplean datos personales en alguna de las etapas de su ciclo de desarrollo y comercialización, ya sea en la fase de entrenamiento y de validación, ya sea en otras etapas posteriores de explotación. Así, por ejemplo, en el ámbito de la salud, de la seguridad, del cálculo del riesgo financiero, etc. No obstante, existen otros muchos sistemas de IA que no los utilizan en ninguna de sus fases de vida, ni en su desarrollo, ni en su explotación, como pueden ser los que se emplean en el ámbito de la geología, la predicción de la climatología, la resistencia de materiales, el diseño industrial, etc. Aunque los requisitos de explicabilidad y transparencia debieran de ser exigibles en cualquier

[7] El anuncio se ha realizado a través de una nota de prensa el día 13 de abril de 2023 y puede consultarse en (aepd.es).

[8] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión).

CC BY SA

DOI: https://doi.org/10.51915/ret.309

sistema de IA[9], en este trabajo se analizarán aquellos que afectan a las personas a través de decisiones automatizadas y que han sido entrenados con datos personales o que los utilizan en alguna de las fases de su ciclo de vida, en un contexto muy concreto, el de las plataformas en línea y motores de búsqueda en línea de muy gran tamaño en el sentido del Reglamento de Servicios Digitales (RSD). Se trata de sistemas de IA que analizan patrones de comportamiento para diseñar publicidad personalizada, ofrecer o seleccionar determinados contenidos o información.

Ha de hacerse referencia en esta introducción a otro factor, que ha condicionado en los últimos años el desarrollo de los sistemas y herramientas del campo de la inteligencia artificial: la cantidad de información personal disponible. Como ya he señalado en otro lugar (Garriga Domínguez, 2015), este hecho nos sitúa por sí mismo 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" (MAYER-SCHÖNBERGER, y CUKIER, 2013: 18). 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 terceros, ya sean operadores públicos o privados. Asimismo, el número creciente de personas, dispositivos y sensores que están conectados por redes digitales ha revolucionado la capacidad de generar, comunicar, compartir y acceder a los datos (TENE, y POLONETSKY, 2012: 63). La definición de *Big Data* incluye ambos elementos: por un lado, la gran cantidad de datos disponibles y, por otro, el conjunto de tecnologías cuyo objetivo es tratar esas grandes cantidades de información (BELTRÁN PARDO y SEVILLANO JAÉN. 2013: 16), 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. El conjunto de tecnologías del ámbito de la IA que se emplean para analizar estas inmensas cantidades de datos, recibe el nombre de «minería de datos» (RAMOS BERNAL, 2012: 186).

Una de las características de muchos de los nuevos sistemas de IA es que utilizan el aprendizaje automático. De acuerdo con la conocida definición de Arthur L. Samuel (SAMUEL, 1983), el proceso de aprendizaje automático de los algoritmos haría referencia *al campo de estudio que da a los computadores la habilidad de aprender algo para lo que no han sido programados expresamente*. Para su desarrollo se necesitan de grandes cantidades de datos de alta calidad. De hecho, muchos de los problemas de sesgo en los sistemas de IA (Vid. O'NEIL, 2017) se deben a datos de entrenamiento de baja calidad, bien porque no son suficientemente diversos, como

[9] Ambos principios se encuentran recogidos en las Directrices éticas para una IA fiable del Grupo independiente de expertos de alto nivel sobre inteligencia artificial, creado por la Comisión Europea en junio de 2018. Asimismo, la Propuesta de Reglamento de Inteligencia Artificial refuerza las obligaciones de transparencia.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

cuando no se incluyen datos de mujeres o de minorías étnicas (Vid. AÑÓN ROIG, 2022), o porque no se cuenta con un volumen suficiente de datos de entrenamiento. Aunque en ocasiones son los propios programadores o desarrolladores quienes introducen sus propios sesgos o prejuicios, en otras se producen fallos porque no se definen correctamente los objetivos del sistema de IA o porque quien debe interpretar los resultados lo hace también de forma sesgada o incorrecta. Precisamente, el tamaño de los datos disponibles en la web, si bien ha permitido a los modelos de aprendizaje profundo alcanzar una alta precisión en aplicaciones PNL, dan lugar a modelos que codifican prejuicios estereotipados y peyorativos en función del género, la raza, la etnia y la discapacidad (BENDER, GEBRU, MCMILLAN-MAJOR y SHMITCHELL, 2021).

Además de los sesgos, que perpetúan los prejuicios y la discriminación (BELLOSO MARTÍN, 2022: 61)[10], otro riesgo de las tecnologías de IA que utilizan *Big Data*, proviene de la posibilidad de extraer patrones de comportamiento y perfiles personales (CRAIG, y LUDLOFF, 2011: 6), haciendo posible una peligrosa y nueva filosofía de la anticipación, cuyo extremo sería el de las predicciones preventivas (KERR y EARLE, 2013: 65). Pueden 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 (LYON, 2014: 101). Y, como ha señalado Soshana Zuboff, el matrimonio formado por la modificación de la conducta y los medios tecnológicos adecuados para automatizar su aplicación es fundamental "para la creación de economías de acción" características de estos operadores (ZUBOFF, 2019: 400). Por otra parte, la elaboración de perfiles y el establecimiento de correlaciones y predicciones permitirá visibilizar "modelos colectivos de comportamiento" (BYUNG-CHUL, 2014: 109) y posibilitará la clasificación social de los individuos y los grupos para la adopción de determinadas decisiones sobre ellos.

En este trabajo se analizará la importancia del principio de transparencia y de las exigencias derivadas del derecho a la protección de datos personales respecto de los sistemas de IA utilizados para determinar la información a la que un usuario concreto de una plataforma va a tener acceso. Un ejemplo, lo encontramos en los servicios que utilizan algoritmos para personalizar las noticias u otros contenidos para cada usuario, pues estos emplearán "parámetros de medición basados en afinidades digitales que delimitan, para el usuario, ventanas de visibilidad que tienen el color de su red social" (CARDON, 2018: 43). Así, cada usuario tendrá acceso a una

[10] Señala Nuria Belloso, que "los sesgos algorítmicos se encuentran en todas las plataformas" y que, en la medida en que todo lo que hacemos se procesa y mediatiza por algoritmos sesgados, deben ofrecerse adecuadas respuestas jurídicas a las amenazas a los derechos fundamentales.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las exigencias de transparencia para los sistemas algorítmicos…
por Ana Garriga Domínguez
Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

información determinada en función de sus intereses, de situación particular o de su estado emocional, que habrán sido previamente identificados por el sistema.

Es importante señalar que, el impacto de los sistemas algorítmicos de moderación de contenidos, de recomendación y los sistemas publicitarios personalizados en el ámbito de determinados servicios digitales, como los motores de búsqueda y las plataformas en línea de muy gran tamaño, no se limita al derecho a la privacidad. Los riesgos derivados de determinadas prácticas pueden afectar, asimismo, a las libertades de expresión e información, a la libertad ideológica o los propios valores democráticos. 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 (BAKSHY, MESSING y ADAMIC 2015: 1130) en las que la decisión sobre los contenidos o sobre cómo se presentan se toma en base a perfiles personalizados, los agentes políticos se ven compelidos a utilizar también estos medios por su eficacia y para conseguir una mayor visibilidad (ECHEVERRÍA, 2013: 175 y ss.). Ahora bien, no es lo mismo el debate de ideas o la publicidad legítima (Vid. GARCÍA MAHAMUT, 2015: 30 y ss.), que la propagación de noticias falsas y los fenómenos de desinformación que utilizan el potencial del *Big Data* y de la micro-segmentación para conseguir sus objetivos económicos o políticos[11]. Las posibilidades actuales de micro-segmentación y manipulación *online* basadas en las tecnologías de *Big Data* e inteligencia artificial hacen que el riesgo para los derechos de las personas sea hoy muy elevado.

Como ha señalado el Supervisor Europeo de Protección de Datos (SEPD) 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"[12]. 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"[13]. En su Informe de enero de 2018, el Grupo Consultivo sobre Ética del Supervisor Europeo de Protección de Datos señalaba, entre las amenazas para la autonomía

[11] 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), en: https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation, *p. 11.*

[12] SEPD. *Opinion 3/2018, on online manipulation and personal data*, adoptada el 13 de marzo de 2018, p.3. Este documento está disponible en la página oficial del Supervisor Europeo de Protección de Datos (edps.europa.eu).

[13] *Ibídem,* p. 7.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

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 o focalización (targeting) y elaboración de perfiles psicográficos[14]; 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[15].

La focalización va a permitir transmitir mensajes específicamente diseñados para promover intereses económicos o comerciales, ideológicos o políticos o de cualquier otra clase. Pues, el *targeting* tiene, como objetivo prioritario, orientar o dirigir al sujeto o a un grupo de personas en un sentido y con una finalidad determinados. Como estos sistemas de IA, como la mayoría de los sistemas automatizados de toma o de ayuda a la decisión, resultan tan complejos y opacos para un usuario medio, el principio de transparencia debe tener un papel central a fin de ayudar a comprender por qué se le ofrecen determinados contenidos y no otros.

El Comité Europeo de Protección de Datos (CEPD) ha identificado una larga una serie de riesgos para los derechos y libertades de los usuarios de las plataformas y medios sociales. La elaboración de perfiles socava la capacidad de las personas "para ejercer el control sobre sus datos personales"[16], aumenta el riesgo de discriminación, utilizando, o no, informaciones sensibles, y de manipulación que podría afectar a cuestiones y procesos políticos, al acentuar vulnerabilidades y emociones negativas afectando a la autonomía, la libertad y a la salud psicológica, en especial en el caso de los menores, pues se puede aprovechar determinados momentos en los que el análisis de la información revele determinados estados emocionales "para dirigir a la persona mensajes específicos y en momentos concretos a los que se espera que sea más receptiva e influir así subrepticiamente en su proceso de pensamiento, sus emociones y su comportamiento"[17].

El desarrollo de la IA permite el perfilado ideológico individual, de la misma forma en la que pueden inferirse perfiles de otras clases, ya sea sobre preferencias de

[14] Ethics Advisory Group. 2018. Report 2018, p.18. El informe puede descargarse de la página oficial del Supervisor Europeo de Protección de Datos (dps.europa.eu).

[15] Ibídem, p. 28.

[16] Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, Versión 2.0, adoptadas el 13 de abril de 2021, p. 7.

[17] *Ibídem*, p. 7.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

DOI: https://doi.org/10.51915/ret.309

consumo, fiabilidad financiera, emocional[18] o, incluso sobre orientación sexual (SARIGOL, GARCÍA y SCHWEITZER, 2014: 105). La elaboración de perfiles en las plataformas sociales permite aplicar técnicas de micro-segmentación para elaborar información política personalizada. Está clara la relación entre la elaboración de perfiles emocionales e ideológicos y las *fake news* y el fenómeno de la desinformación a través de la red y la institución de la opinión pública libre (ALCARÁZ RAMOS, 2020). En consecuencia, se produce una estrecha conexión entre la garantía de la privacidad de las personas y el ejercicio de estas libertades, que están en la base del sistema democrático.

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 focalización política en las elecciones presidenciales de Estados Unidos de 2016 y en el referéndum sobre la permanencia en la Unión Europea del Reino Unido[19]. 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"[20]. Pero, la libre circulación de opiniones e informaciones se ve obstaculizada por *bots* y noticias falsas, pero también, cuando se aplican «burbujas de filtro», que a través de filtros invisibles, nos aísla sin percibirlo y el sistema se aprovecha del incentivo psicológico que supone el sesgo de confirmación (ALCOTT, y GENTZKOW, 2017: 211). 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" (PARISIER, 2017: 18). Como consecuencia de estas prácticas, también la libertad ideológica podrá resultar afectada. Su papel es esencial en un Estado democrático y presupuesto del derecho de participación, del pluralismo político (XIOL RÍOS, 2001: 18 y ss.) y "requisito de funcionamiento del Estado democrático" (ROLLNERT LIERN, 2002: 70). Para garantizar este elemento negativo de la libertad ideológica y de

[18] A través de las 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" (MAYER-SCHÖNBERGER y CUKIER. 2013: 116 - 117.

[19] 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".*

[20] STC 173/1995, de 21 de noviembre.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

conciencia[21], tanto el RGPD como la LOPDGDD[22] prohíben, como regla general, aunque con determinadas excepciones, el tratamiento de los datos personales que revelen las opiniones políticas[23], las convicciones religiosas o filosóficas (artículos 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 hace posible inferir las convicciones ideológicas y de conciencia de una persona sin que esta las haya hecho públicas, pudiendo "hallarse correlaciones que indiquen algo sobre la salud, las convicciones políticas, las creencias religiosas o la orientación sexual de las personas"[24].

Puede constatarse que los instrumentos del RGPD son insuficientes ante esta problemática y, en tanto no se apruebe definitivamente el Reglamento de IA, el Reglamento de Servicios Digitales debería servir para afrontar y mitigar los riesgos y problemática descritos. Sus normas suponen un refuerzo a las garantías que existían hasta ahora en el ordenamiento jurídico europeo para combatir éstos y otros problemas que ocasionan los sistemas de publicidad *online* y los sistemas de recomendación y selección de contenidos de los grandes operadores en la web. En este trabajo se prestará atención a las que buscan garantizar una mayor transparencia de los algoritmos usados con esos fines; si bien, como no es necesario explicar, su contenido es mucho más amplio y regula otras muchas cuestiones.

2.- Las garantías derivadas del principio de transparencia en el reglamento general de protección de datos

2.1.- Decisiones automatizadas y elaboración de perfiles

Este tema será tratado de forma breve, destacando aquellos aspectos esenciales para la temática de este trabajo, ya que su análisis en profundidad fue abordado en

[21] Vid. STC 46/2001 de 15 febrero.

[22] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[23] Sobre los estrictos requisitos que exige su tratamiento, se pronunció el Tribunal Constitucional en su STC 76/2019, de 22 de mayo, que anuló el apartado 1 del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que regulaba la recopilación por los partidos políticos de datos personales relativos a las opiniones políticas de los ciudadanos.

[24] El CEPD 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, nº 15, pp. 5802–5805. Dicho estudio, *"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"*. (*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* del GT29, Adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 17).

CC BY SA

DOI: https://doi.org/10.51915/ret.309

dos estudios precedentes a los que me remito (GARRIGA DOMÍNGUEZ, 2018 y 2021). Por otra parte, en mi opinión, el derecho a la protección de datos personales se presenta como un instrumento válido, pero insuficiente, frente a las técnicas de difusión de noticias falsas, cuya viralización se produce "a través de las redes sociales como Facebook o Twitter en lo que se ha venido a bautizar como «cascada informativa" (PAUNER CHULVI, 2018: 302) y el fenómeno de la desinformación y por ello resultaba urgente la aprobación del Reglamento de Servicios Digitales para complementar, en el ámbito de las plataformas que operan en la red, en conjunto de obligaciones y garantías para los derechos fundamentales que propiciaran un entorno en línea seguro y confiable.

El artículo 22 del RGPD, establece 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*. Se aplica tanto a la elaboración de perfiles como a la adopción de decisiones automatizadas, estén o no basadas en perfiles. El artículo 22 del RGPD contiene una prohibición general de tomar decisiones individuales basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos o efectos significativamente similares, si bien existen excepciones a esta norma general y, dichas excepciones cuando se apliquen, exigirán la adopción de medidas específicas para garantizar los derechos y libertades del interesado, así como sus intereses legítimos[25]. La aplicabilidad del artículo 22 dependerá de que se produzcan o se puedan derivar esas consecuencias relevantes para la persona; es decir, cuando produzca efectos jurídicos que afecten al interesado (por ejemplo, afecte a sus derechos, se le deniegue una prestación, produzca efectos en un contrato en el que sea parte) o le afecte significativamente de modo similar, por lo que debe ser suficientemente importante, como por ejemplo, que se le deniegue un crédito, que le afecte a su acceso a determinados servicios, en el acceso o promoción en el empleo, etc. No obstante, en determinados casos, es posible la elaboración de perfiles o la adopción de decisiones automatizadas y su licitud dependerá de que cuenten con una base de legitimación válida y cumplan los principios relativos al tratamiento. No nos encontramos ante un derecho absoluto, estableciéndose en el RGPD una serie de excepciones: cuando la decisión esté autorizada por el Derecho de la Unión o de los Estados miembros; cuando sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; o cuando se base en el consentimiento explícito del interesado. En estos dos últimos supuestos el art. 22.3 exige que el responsable del tratamiento establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado y se le garantice: el derecho a

[25] *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* del GT29, Adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 16.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

obtener intervención humana por parte del responsable; el derecho a expresar su punto de vista y el derecho a impugnar la decisión.

Finalmente, en el art. 22 se establece una limitación en razón de la naturaleza de los datos personales prohibiéndose la adopción de decisiones automatizadas basadas en datos sensibles o especialmente protegidos (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales) salvo que el interesado haya prestado su consentimiento explícito y esta posibilidad no esté prohibida por el Derecho de la Unión o de los Estados miembros 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. En ambos casos deberán tomarse medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

2.2.- La importancia de los principios de transparencia y de responsabilidad proactiva del RGPD en los sistemas de IA

El RGPD exige que en cualquier tratamiento de datos personales se respeten tanto los principios relativos al tratamiento, como que este cuente con una base de legitimación adecuada[26]. El artículo 5 del RGPD regula los principios básicos que deberán respetarse en cualquier tratamiento de datos personales. Sin embargo, aunque todos ellos deben exigirse, en el contexto de los sistemas de IA que adoptan decisiones, contenidos o recomendaciones, con fines de publicidad o comerciales u otros diferentes, ocupan un papel destacado dos de ellos: el principio de transparencia y el de responsabilidad proactiva.

El principio de responsabilidad proactiva se encuentra desarrollado en el artículo 24 del RGPD, al establecer la obligación general del responsable del tratamiento de aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder

[26] Sobre la inadecuación de la letra b) del artículo 6.1 del RGPD (ejecución de un contrato) como base de legitimación para la publicidad de comportamiento en línea se ha pronunciado el CEPD en sus Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados, p. 16 y ss. Señala el CEPD que, "como regla general, el tratamiento de datos personales con fines de publicidad del comportamiento no puede considerarse necesario para la ejecución de un contrato de servicios en línea" ya que resulta muy difícil demostrar "que el contrato no pueda ejecutarse debido a la ausencia de anuncios publicitarios de comportamiento". Por otra parte, "el artículo 6, apartado 1, letra b), no puede servir de fundamento jurídico para la publicidad del comportamiento en línea por el mero hecho de que este tipo de publicidad financie de manera indirecta la prestación del servicio. Aunque este tipo de tratamiento puede respaldar la prestación del servicio, ello no basta de por sí para determinar que resulta necesario para ejecutar el contrato en cuestión".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.309

demostrar que el tratamiento es conforme con el RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. Supone un cambio de paradigma que exige pasar de un sistema de protección reactivo frente al incumplimiento a un modelo preventivo y proactivo (LORENZO CABRERA, 2018: 123-125). Va a exigir un enfoque desde el riesgo para determinar la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado[27]. Será necesario realizar una evaluación objetiva atendiendo a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos en el proceso de micro-segmentación. Por lo tanto, de forma previa a la focalización habrá de valorarse, por aquellos que intervengan en las diferentes fases del procedimiento, si dicho tratamiento se va a servir de datos especialmente protegidos o si va a implicar un *"alto riesgo"* para las personas y sus derechos, que exijan la realización de una EIPD (Evaluación de Impacto relativa a la Protección de Datos). Este sería el caso de anuncios dirigidos a personas vulnerables, ya que es posible que surjan "riesgos adicionales en función de los fines de la campaña publicitaria y su carácter intrusivo, o de si la focalización implica el tratamiento de datos personales observados, inferidos o derivados"[28].

Por otra parte, como una de las características de estos procesos es, que suelen ser opacos para las personas, o a éstas, les cuesta comprender su funcionamiento y la relevancia de sus aplicaciones y consecuencias, el cumplimiento del principio de transparencia resulta capital. En el RGPD, las referencias al principio de transparencia son constantes garantizando que, de forma sencilla, fácilmente accesible y en un lenguaje claro y sencillo, se facilite al interesado toda la información relevante para él en el proceso de tratamiento de sus datos. Esta obligación es especialmente pertinente *"en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea"* (Considerando 58).

La exigencia de transparencia debe ser configurada como *"un derecho prestacional que requiere una actuación positiva por parte de las autoridades públicas" (TOMÁS MALLÉN, 2015: 832 y ss.)* y se conecta con el establecimiento de un contenido pormenorizado del derecho de información y de las correlativas obligaciones informadoras del responsable del tratamiento. Así se recoge en el artículo 13 del

[27] Este enfoque desde el riesgo es también el adoptado en la Propuesta de Reglamento de Inteligencia Artificial. La Propuesta clasifica los sistemas de IA en cuatro niveles atendiendo a su posible riesgo, en función de la gravedad del daño y de su probabilidad.

[28] Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, Versión 2.0, adoptadas el 13 de abril de 2021, p. 34.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

RGPD[29], que obliga al responsable del tratamiento a adoptar las medidas oportunas para facilitar al interesado toda información relevante relativa al tratamiento de sus datos personales incluida la existencia de decisiones automatizadas y la elaboración de perfiles, así como *"información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento para el interesado"*. Igualmente, el principio de transparencia obliga al responsable del tratamiento a garantizar que se le informa, aún cuando los datos no se hayan obtenido directamente del interesado, en los términos previstos en el artículo 14 y a garantizar el derecho de acceso, en el artículo 15, a la información relativa a la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento.

Por último, es necesario destacar que la obligación de transparencia se configura como "una expresión del principio de lealtad en relación con el tratamiento de los datos personales plasmado en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea"[30]; pues, cualquier tratamiento de datos personales deberá de ser lícito y leal de forma que al interesado le ha de quedar totalmente claro que se están recogiendo y utilizando sus datos y en la medida en que éstos son o serán tratados de forma que, como señala el Comité Europeo de Protección de Datos, las personas no se vean sorprendidas "en un momento posterior del uso que se ha dado a sus datos personales"[31]. Señala COTINO, asimismo, el principio de transparencia deberá aplicarse a los datos de entrenamiento y también a los datos de entrada para su funcionamiento, validación y prueba; pues, "se trata de un elemento clave que incide directamente en la calidad y robustez del sistema, así como respecto de la posibilidad de controlar sesgos, errores o posibles discriminaciones" (COTINO HUESO, 2023: 33).

Al igual que ocurre con el enfoque desde el riesgo, las exigencias de transparencia también se recogen en la Propuesta de Reglamento sobre IA, estableciéndose "normas armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los

[29] El incumplimiento del principio de transparencia, entre otros requisitos, ha llevado a la *Irish Data Protection Authority* a sancionar a Meta el pasado enero. Sus dos decisiones sancionadoras fueron el resultado de investigaciones basadas en reclamaciones sobre las actividades de Facebook e Instagram, en particular en relación con la legalidad y la transparencia del tratamiento para la publicidad basada en el comportamiento. La Autoridad irlandesa impuso a Meta una multa de 210 millones de euros en la decisión sobre Facebook y de 180 millones de euros en la decisión sobre Instagram. El comunicado, *"Facebook and Instagram decisions: "Important impact on use of personal data for behavioural advertising"*, puede consultarse en la página oficial del Comité Europeo de Protección de Datos (EDPD, por sus siglas en inglés) del día 12 de enero de 2023 (edpb.europa.eu/news).

[30] Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, Adoptadas el 29 de noviembre de 2017. Revisadas por última vez y adoptadas el 11 de abril de 2018, p. 5.

[31] *Ibídem*, p. 8.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

sistemas de categorización biométrica, así como a los sistemas de IA usados para generar o manipular imágenes, archivos de audio o vídeos" (artículo 1) y exigiendo para los sistemas de IA de Alto Riesgo que se diseñen y desarrollen "de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida" (artículo13). Estas exigencias de transparencia en la IA se indican también en el Libro Blanco sobre la inteligencia artificial de la Comisión, de 19 de febrero de 2020, ya que "la falta de transparencia (opacidad de la IA) hace difícil detectar y demostrar los posibles incumplimientos de la legislación, especialmente las disposiciones legales que protegen los derechos fundamentales, imputan responsabilidades y permiten reclamar una indemnización"[32].

3.- Obligaciones específicas para las plataformas en línea y motores de búsqueda de muy gran tamaño[33] en el Reglamento (UE) 2022/2065, de 19 de octubre, de Servicios Digitales (RSD). Especial referencia a las obligaciones de transparencia algorítmica

3.1.- Un Reglamento para crear un entorno en línea seguro y frenar la difusión de desinformación y manipulación en línea

El desarrollo de Internet y la proliferación de servicios en la red supuso el incremento del número y clase de servicios disponibles: acceso a toda clase de información y documentación en cualquier lugar del mundo, posibilidad de comunicarse y relacionarse con un número ilimitado de personas, acceso a nuevas formas de ocio, posibilidad de adquirir servicios o bienes de cualquier clase a través del comercio electrónico, etc. Su desarrollo modificó hábitos y costumbres de ocio, laborales y profesionales, como consumidores o en nuestras relaciones como ciudadanos con las diferentes administraciones. Internet ha transformado también las formas de actuación de las empresas y de las entidades públicas e incluso puede afirmarse que ha supuesto la desaparición de los conceptos de espacio y tiempo en las comunicaciones (CAMPUZANO TOMÉ, 2002: 17). Se desarrollaron nuevos servicios de comunicación e información, aunque, al mismo tiempo, se amplificaron los riesgos y ataques para los derechos de las personas. Internet permite fácilmente a los usuarios elaborar informaciones, opiniones y contenidos de toda clase que pueden compartir con otros grupos de personas, divulgándolos a escala planetaria. Por ello, brinda un gran potencial para la promoción de la democracia y la diversidad cultural y el ejercicio de las libertades de expresión e información. Sin embargo, existe una necesidad objetiva de controlar la red, pues es utilizada también para la

[32] Anteriormente, en la Comunicación de la Comisión de 8 de abril de 2019 "Generar confianza en la inteligencia artificial centrada en el ser humano", se identificaba este concepto como uno de los siete requisitos esenciales para lograr una IA fiable.

[33] VLOP y VLOSE por sus siglas en inglés (*Very Large Online Platforms* y *Very Large Online Search Engines).*

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

comisión de delitos, como mensajero implacable de la difamación y el acoso, en especial a mujeres y grupos vulnerables o minorías, para atentar contra la vida privada de las personas, supone riesgos específicos para los derechos de la infancia, facilita los ilícitos contra la propiedad intelectual, etc.

Entre los objetivos del Reglamento de Servicios Digitales destaca el de crear un entorno en línea seguro, predecible y confiable, en el que las personas puedan ejercer sus derechos fundamentales, en particular, la libertad de expresión e información. Así se recoge en el Considerando 3 y a lo largo de toda su parte expositiva. El legislador europeo es muy consciente del papel que juega la publicidad en línea en el discurso político y en otros ámbitos sensibles como puede ser el de la salud pública o en la propagación del discurso del odio, señalando que la publicidad en línea "puede contribuir a generar riesgos significativos, desde anuncios publicitarios que sean en sí mismos contenidos ilícitos hasta contribuir a incentivar económicamente la publicación o amplificación de contenidos y actividades en línea que sean ilícitos o de otro modo nocivos"[34]. Como ya se ha señalado, la aplicación de la IA en estos ámbitos permite el perfilado ideológico individual y, a través de las técnicas de focalización, podrá elaborarse información política personalizada. De esta forma, 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 concretos para influir en su conducta (BARBU, BARBU, 2014: 46) y, como ha señalado el CEPD, esta práctica tendrá consecuencias negativas para el pluralismo político y el debate público de ideas, pero existirán otros riesgos, de discriminación utilizando, o no, informaciones sensibles y, asimismo, un riesgo real de manipulación, que podría afectar a cuestiones y procesos políticos, acentuando vulnerabilidades y emociones negativas[35].

Son varios los instrumentos que el RSD utiliza para lograr estos objetivos, desde la prohibición de la publicidad dirigida a menores, hasta una serie de medidas para garantizar a los usuarios un mayor control sobre el uso de sus datos personales. Refuerza el principio de transparencia y establece obligaciones para los prestadores de los servicios de informar sobre cuándo y en nombre de quién se presenta la publicidad, así como los principales parámetros utilizados para determinar que se les va a presentar publicidad específica, que ofrezca explicaciones reveladoras de la lógica utilizada con ese fin, también cuando se base en la elaboración de perfiles. Además de estas obligaciones generales de transparencia, se establecen obligaciones específicas para las plataformas en línea y buscadores de muy gran

[34] Considerando 52.

[35] Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, Versión 2.0, adoptadas el 13 de abril de 2021, p. 7.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las exigencias de transparencia para los sistemas algorítmicos…
por Ana Garriga Domínguez
Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

tamaño, con un número de destinatarios activos en la Unión de 45 millones o superior de promedio mensual. La razón del establecimiento de este conjunto de obligaciones particulares está clara: su relevante papel dado su alcance expresado en el número de destinatario de servicio, "para facilitar el debate público, (…) la difusión de información, opiniones e ideas y para influir en la forma en que los destinatarios obtienen y comunican información en línea"[36].

En el Capítulo III se regulan las obligaciones de diligencia debida para crear un entorno en línea transparente y seguro y se establecen las obligaciones adicionales para las plataformas en línea y las exigencias específicas para aquellas de muy gran tamaño. En los artículos 23 y siguientes se dispone la obligación de informar sobre el uso de medios automáticos con fines de moderación de contenidos. También se refuerzan, en los términos que veremos seguidamente, los requisitos de transparencia sobre la publicidad en línea, con especial atención a la transparencia de sus algoritmos.

Otra novedad, siguiendo la estela del RGPD, es el enfoque desde el riesgo que se concretará, para las plataformas de muy gran tamaño, en la obligación de evaluación de los riesgos sistémicos. Entre estos riegos sistémicos, habrán de considerarse necesariamente los riesgos de difusión de contenido ilícito a través de sus servicios o cualquier efecto negativo para el ejercicio de los derechos fundamentales a la vida privada y familiar, la libertad de expresión e información, la prohibición de la discriminación y los derechos del niño. Así mismo, deberán evaluarse los riesgos de manipulación deliberada de su servicio que pueda producir un *"un efecto negativo real o previsible sobre la protección de la salud pública, los menores, el discurso cívico o efectos reales o previsibles relacionados con procesos electorales y con la seguridad pública"* (artículo 26). Estos riesgos podrían derivarse, como se indica en el Considerando 58, de la creación de cuentas falsas, del uso de *bots* u otros comportamientos, total o parcialmente automatizados, con el resultado de una difusión rápida y extendida de información que constituya un contenido ilícito o incompatible con las condiciones de una plataforma. El RSD es consciente de que el fenómeno de la desinformación, la difusión de contenidos ilícitos o noticias falsas es complejo y en su propagación intervienen, no solo las noticias falsas, sino también las cuentas falsas y *bots,* que sirven para amplificar "la actividad e intensidad de los servicios" (LANIER, 2018: 77). Pues, como ya se ha indicado, las empresas que producen estos contenidos 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 "porque eso es lo que impulsa la influencia y los ingresos por publicidad" (HOLIDAY, 2013: 290-291). Este fenómeno se ve potenciado porque su

[36] Considerando 53.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

contenido puede ser retransmitido entre los usuarios sin necesidad de un filtrado de verificación de hechos o juicio editorial significativo por parte de terceros.

Precisamente, para reducir estos riesgos se establecen refuerzan las obligaciones de diligencia[37], que impliquen la adopción de medidas correctoras adecuadas, que pueden implicar mejoras en el diseño y en el funcionamiento de los sistemas de moderación, de los sistemas algorítmicos de recomendación e de las interfaces en línea con el fin de salvaguardar el orden público y los derechos de las personas. También se prohíbe manipular las elecciones de los usuarios mediante los denominados *patrones oscuros,* en los términos que veremos seguidamente.

3.2.- Obligaciones de transparencia para los motores de búsqueda (VLOSE) y las plataformas en línea de muy gran tamaño (VLOP). Especial referencia a las obligaciones de transparencia algorítmica

El RSD propone un modelo de regulación para delimitar "el alcance de las libertades de empresa e informativas de las plataformas", que "parte de las acciones y autorregulaciones ya adoptadas por las plataformas contra la desinformación y las reorienta e impulsa hacia los objetivos necesarios" (COTINO HUESO, 2022: 236). Dentro del conjunto de obligaciones de diligencia debida para crear un entorno en línea transparente y seguro del Capítulo III del RSD, destacan las obligaciones de transparencia informativa de los prestadores de servicios intermediarios y de alojamiento de datos, excluyendo a aquellos que sean microempresas o pequeñas empresas. Estas exigencias de transparencia se aplican de forma particular a las actividades de moderación de contenidos realizada por iniciativa propia del prestador de servicios en la red incluyendo los sistemas automatizados de moderación. En concreto, el artículo 15 dispone que estos servicios habrán de publicar como mínimo una vez al año, informes claros y fácilmente comprensibles sobre cualquier actividad de moderación de contenidos que hayan realizado durante el período pertinente. Estos informes deberán incluir, en particular, la siguiente información:

- El número de órdenes recibidas de las autoridades de los Estados miembros, categorizadas según el tipo de contenido ilícito de que se trate, el Estado miembro que haya dictado la orden y el tiempo medio necesario para informar a dicha autoridad;

- Para los prestadores de servicios de alojamiento de datos, el número de notificaciones enviadas de conformidad con el artículo 16, según el tipo de contenido

[37] Obligaciones de diligencia para los prestadores de servicios de alojamiento de datos, en orden a prevenir o detectar contenidos y actividades ilegales, ya existían en la Directiva 2000/31/CE y así lo venían exigiendo los tribunales españoles en aplicación de la ley 34/2002, de 11 julio 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Por todas, sentencia de la Sala 1ª del Tribunal Supremo 773/2009, de 9 de diciembre.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

presuntamente ilícito, el número de notificaciones enviadas por alertadores fiables, así como las actuaciones resultantes de dichas notificaciones, el número de notificaciones tratadas únicamente por medios automatizados y el tiempo medio necesario para adoptar medidas;

- Para los prestadores de servicios intermediarios, se exige que se recoja la información significativa y comprensible sobre la actividad de moderación de contenidos realizada por iniciativa propia del prestador, incluido el uso de herramientas automatizadas. Asimismo, el número y el tipo de medidas adoptadas para formar y asistir a los moderadores del servicio, así como aquellas medidas "que afecten a la disponibilidad, visibilidad y accesibilidad de la información proporcionada por los destinatarios del servicio y a la capacidad de los destinatarios para proporcionar información a través del servicio, y otras restricciones conexas del servicio";

- En el caso de los prestadores de servicios intermediarios, el número de reclamaciones recibidas a través de sus sistemas internos de gestión de reclamaciones y, para los prestadores de plataformas en línea, la base de dichas reclamaciones, las decisiones adoptadas en relación con dichas reclamaciones, con especificación del tiempo medio necesario para adoptar dichas decisiones, así como el número de decisiones revocadas;

- Cuando se utilicen medios automatizados con fines de moderación de contenidos, deberá señalarse este hecho, incluyendo una descripción cualitativa, con referencia a los fines concretos y específicos del sistema, los indicadores de la precisión y la posible tasa de error de dichos medios automatizados, así como, las salvaguardias aplicadas.

Como se ve, se trata de un conjunto de medidas que pretenden garantizar la rendición de cuentas de los prestadores del servicio y de alerta del uso de sistemas automatizados de decisión.

Estas obligaciones se complementan con las establecidas en la Sección 3 para las plataformas en línea[38]. Para el tema objeto de este trabajo, destacan dos: la prohibición del uso de patrones oscuros del artículo 25 y la especificación del contenido de la información que se debe facilitar al destinatario del servicio cuando se presente publicidad en línea, del artículo 26.

Si bien, la prohibición de los patrones oscuros, es decir, aquellas "interfaces de usuario diseñadas para influir, a través de manipulaciones psicológicas y de forma

[38] Las obligaciones de transparencia informativa del artículo 15 se completan para los prestadores de plataformas en línea en el artículo 24 que exige información adicional sobre el número, los resultados, porcentaje y tiempo medio para los litigios sometidos a los órganos de resolución extrajudicial de litigios a que se refiere el artículo 21 y el número de suspensiones impuestas en virtud del artículo 23.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

encubierta, en las elecciones del interesado, al menos, con relación al tratamiento de sus datos personales"[39], se entendía una exigencia derivada de los principios de lealtad y transparencia del artículo 5.1.a) del RGPD[40], el legislador europeo ha considerado necesario incluir la prohibición los prestadores de servicios de plataformas en línea de diseñar, organizar o gestionar "sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio[41] o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas"[42], ya que los patrones oscuros se utilizan para que el usuario no proteja adecuadamente su privacidad, pero pueden emplearse también con otros fines.

Respecto de las obligaciones de transparencia en relación con la publicidad en línea, se exige a las plataformas que, por cada anuncio publicitario concreto presentado a cada destinatario específico, se deberá proporcionar a los destinatarios del servicio determinada información para que "sean capaces de identificar, de manera clara, concisa e inequívoca y en tiempo real", que la información es un anuncio publicitario; en nombre de quien se presenta el anuncio y quien ha pagado el anuncio, si es distinta de la aquella y la información sobre los principales parámetros utilizados para determinar el destinatario a quien se presenta el anuncio publicitario y acerca de cómo cambiar esos parámetros.

En este caso, las medidas de transparencia responden a la necesidad de clarificar el funcionamiento opaco y, generalmente, poco comprensible de cómo se realiza esta clase de publicidad, de cómo se produce la focalización y la selección del momento en que esta se ofrece. Además, en el RSD se presta especial atención a la publicidad segmentada diseñada en base a los intereses y vulnerabilidades de los usuarios por

---

[39] Guía de Protección de Datos por Defecto de la Agencia Española de Protección de Datos (AEPD), p. 20.

[40] Así lo ha entendido la AEPD (Vid. *Dark patterns: Manipulación en los servicios de Internet*. 2022). Más ampliamente, de acuerdo con la definición del CEPD, los "patrones oscuros" se consideran interfaces y experiencias de usuario implementadas en plataformas de medios sociales que llevan a los usuarios a tomar decisiones no intencionadas, involuntarias y potencialmente perjudiciales en relación con el tratamiento de sus datos personales. Los patrones oscuros pretenden influir en el comportamiento de los usuarios y pueden obstaculizar su capacidad para proteger eficazmente sus datos personales y tomar decisiones conscientes. En *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them.* En especial p. 3 y ss.

[41] Un conocido caso de manipulación emocional fue el que se realizó a lo largo de una semana durante el año 2012 en Facebook. En KRAMER, A., GUILLORY, J. E. y HANCOCK, J. T. 2014. *"Experimental evidence of massive-scale emotional contagion through social networks",* Proceedings of the National Academy of Sciences of Unites States of America, vol. 11, nº 24.

[42] Ejemplos reales de cómo las plataformas sociales y otros operadores utilizan el diseño de sus interfaces para manipular o engañar al usuario, alguno de ello durante sancionado por los tribunales, pueden consultarse en LACORT, J. 2018. *"Los 'dark patterns' del diseño: así hackean tu cerebro webs y aplicaciones para sacarte más dinero o retener tu atención".* Xataka, 2018. La información completa puede consultarse en la web de la revista (xataka.com) y fue publicada el día 15 de mayo de 2018.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Págs. 137-164
DOI: https://doi.org/10.51915/ret.309

sus potenciales efectos negativos, prohibiéndose la elaboración de perfiles, en el sentido del Reglamento General de Protección de Datos, basada en categorías de datos especialmente protegidos de acuerdo con lo dispuesto en su artículo 9.1.

Estas obligaciones se completan en la Sección 5 con medidas adicionales de transparencia para las VLOP y los VLOSE en el artículo 39. A estos operadores se les obliga, cuando presenten publicidad en sus interfaces a recopilar y hacer públicas en una sección específica de su interfaz, a través de una herramienta de búsqueda fiable que permita realizar consultas en función de múltiples criterios, y mediante interfaces de programación de aplicaciones, un repositorio que deberá estar disponible durante "todo el tiempo en el que presenten un anuncio y hasta un año después de la última vez que se presente el anuncio en sus interfaces en línea", debiendo asegurarse "de que el repositorio no contenga ningún dato personal de los destinatarios del servicio a quienes se haya o se pueda haber presentado el anuncio y harán todos los esfuerzos que resulten razonables para garantizar que la información sea exacta y completa". En dicho repositorio se deberá recoger la siguiente información: el contenido del anuncio publicitario, incluidos el nombre del producto, servicio o marca y el objeto del anuncio; la persona física o jurídica en cuyo nombre se presenta el anuncio publicitario y la que lo haya pagado cuando sea diferente de la anterior; el período de tiempo durante el que se haya presentado el anuncio; cuando el anuncio esté destinado a presentarse en particular a uno o varios grupos concretos de destinatarios, deberá informarse de los parámetros principales utilizados para tal fin, incluidos, aquellos utilizados para excluir a uno o más de esos grupos concretos; las comunicaciones comerciales publicadas en las plataformas en línea de muy gran tamaño, que deberán estar identificadas de acuerdo con lo recogido en artículo 26.2 y, finalmente, el número total de destinatarios del servicio alcanzados, desglosado por Estado miembro para el grupo o grupos de destinatarios a quienes el anuncio estuviera específicamente dirigido.

Las obligaciones de transparencia algorítmica se extienden asimismo a los sistemas de recomendación debiendo las plataformas informar, de forma sencilla y comprensible, acerca de cuales son "los parámetros principales utilizados en sus sistemas de recomendación, así como cualquier opción a disposición de los destinatarios del servicio para modificar o influir en dichos parámetros principales". Como mínimo, el artículo 27 determina que se deberán proporcionar al destinatario del servicio, con el fin de explicarle por qué se le recomienda una determinada información, "los criterios más significativos a la hora de determinar la información sugerida al destinatario del servicio", y "las razones de la importancia relativa de dichos parámetros". Las obligaciones de transparencia para los sistemas de recomendación, se completan para las VLOP y los VLOSE en el artículo 38. Estos prestadores deberán incluir en sus sistemas de recomendación al menos una opción, para cada uno de sus sistemas, que no se base en la elaboración de perfiles en el sentido del artículo 4 del RGPD.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

Para los motores de búsqueda y las plataformas en línea de muy gran tamaño, el RSD impone obligaciones adicionales de gestión de riesgos sistémicos que atañen, tanto a la necesidad de realizar una evaluación de riesgos, "que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios", como a la aplicación de medidas de reducción de riesgos razonables, proporcionadas y efectivas para dichos riesgos sistémicos (artículo 35).

Entre los riesgos sistémicos, el artículo 35 determina que necesariamente deberán incluir las evaluaciones se encuentran los siguientes:

- la difusión de contenido ilícito a través de sus servicios;

- cualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales, en particular los relativos a la dignidad humana, al respeto de la vida privada y familiar, a la protección de los datos de carácter personal, a la libertad de expresión e información, incluida la libertad y el pluralismo de los medios de comunicación, a la no discriminación, a los derechos del niño y a un nivel elevado de protección de los consumidores;

- cualquier efecto negativo real o previsible sobre el discurso cívico y los procesos electorales o sobre la seguridad pública;

- cualquier efecto negativo real o previsible en relación con la violencia de género, la protección de la salud pública y los menores, así como las consecuencias negativas graves para el bienestar físico y mental de la persona.

Entre los factores que imperiosamente habrán de tener en cuenta en sus evaluaciones se encuentra la necesidad de prestar atención al diseño de sus sistemas de recomendación y de cualquier otro sistema algorítmico pertinente, a sus sistemas de moderación de contenidos a las prácticas del prestador relacionadas con los datos, a los sistemas de selección y presentación de anuncios y, finalmente, a las condiciones generales aplicables y su ejecución. Asimismo, será necesario que se analice en qué medida los riesgos sistémicos pueden verse influidos y de qué manera, por "la manipulación intencionada de su servicio, en particular por medio del uso no auténtico o la explotación automatizada del servicio, así como la amplificación y la difusión potencialmente rápida y amplia de contenido ilícito y de información incompatible con sus condiciones generales" (apartado 3 del artículo 34). Si el algoritmo es el que nos indica qué es lo que queremos realmente, qué necesitamos, a quién queremos seguir o qué noticias son las que nos interesan y

CC BY SA

DOI: https://doi.org/10.51915/ret.309

atañen, es lógico que el RSD imponga obligaciones de evaluación de riesgo desde el diseño, en especial, ante la posibilidad de manipulación intencionada[43].

Para evaluar el grado de cumplimiento de las obligaciones establecidas en el Capítulo III del RSD, así como las derivadas de los códigos de conducta en los que sean parte a las VOLP y los VLOSE habrán de someterse a auditorías anuales a su costa.

Por último, se refuerza la transparencia confiriendo, al coordinador de servicios digitales y a la Comisión, poderes de escrutinio y acceso a los datos necesarios para hacer un seguimiento de cumplimiento de las obligaciones sistémicas previstas en el mismo. Para ayudar en las funciones de ejecución y supervisión de la Comisión, se ha creado el European Centre for Algorithmic Transparency (ECAT). Entre sus funciones principales se encuentran la de análisis de la transparencia, evaluación de riesgos y propuesta de nuevos enfoques transparentes y mejores prácticas en este ámbito con el fin de mejorar la comprensión de cómo funcionan los algoritmos. Para lograr este objetivo realizará, tanto tareas de evaluación y supervisión, como de investigación y prevención. Le corresponderá trabajar para identificar los riesgos sistémicos asociados a los VLOP y VLOSE, para la propuesta de metodologías para garantizar algorítmicos transparentes y responsables o el estudio del impacto social a largo plazo de los algoritmos[44].

4.- Conclusión

El fenómeno de la desinformación no es nuevo, las teorías de la conspiración, los rumores sin verificar y los bulos ya existían antes de Internet y del desarrollo de las plataformas sociales. Sin embargo, la arquitectura y el modelo de negocio de las plataformas en línea facilita la diseminación de contenidos ilícitos de forma exponencial multiplicando su daño. El propio diseño de los sistemas de IA y de los algoritmos de los sistemas automáticos de recomendación, de selección de contenidos o de publicidad en línea explotan vulnerabilidades y permiten un extenso conocimiento sobre los intereses, gustos, opiniones ideológicas y estados emocionales de los destinatarios de los servicios. Se utilizan filtros burbuja, que

[43] El riesgo de manipulación intencionada ya fue señalado, entre otros, por el CEPD, pues, aprovechando determinados momentos en los que el análisis de la información revele estados emocionales determinados, se pueden *"dirigir a la persona mensajes específicos y en momentos concretos a los que se espera que sea más receptiva e influir así subrepticiamente en su proceso de pensamiento, sus emociones y su comportamiento"* (Directrices 8/2020 sobre la focalización de los usuarios de medios sociales 2021, 7.). Por otra parte, el reconocimiento de emociones es posible, en especial con el uso de tecnologías biométricas y pueden utilizarse para manipular a las personas. Vid. Dictamen conjunto 5/2021 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) del 18 de junio de 2021.

[44] Pueden consultarse sus funciones y misión en European Centre for Algorithmic Transparency (disponible en: algorithmic-transparency.ec.europa.eu).

DOI: https://doi.org/10.51915/ret.309

explotan el sesgo de confirmación, limitando la 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[45].

Los procesos y los sistemas tecnológicos que confluyen en este fenómeno tan complejo son de difícil compresión para el usuario medio y su funcionamiento es poco transparente. 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. Y, si bien es cierto que los sucesivos 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[46], éstas se han mostrado claramente insuficientes. Por ello, resultaba urgente que se establecieran por el legislador europeo obligaciones concretas de transparencia y de rendición de cuentas para los operadores que explotan los procesos de perfilado que permiten condicionar la conducta de las personas, limitar sus opciones informativas o potenciar la desinformación. 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 su significado y quién decide bajo qué circunstancias esas categorías serán decisivas (LYON, 2014: 186).

En la medida en que en los servicios de los operadores en línea, no es el usuario quien elige cómo relacionarse con los demás, sino que es "el proveedor del servicio el que a través del ejercicio de *default power* determina a su antojo los detalles de ese mundo compartido" (IPPOLITA, 2012: 143), el RSD impone claras obligaciones y exige un elevado grado de responsabilidad a "los actores de ecosistema (digital) que

[45] Por su negativa influencia en la salud mental de niños y adolescentes, el distrito de la escuela pública de Seattle presentó una demanda judicial colectiva contras las principales empresas de redes sociales por crear aplicaciones que explotan sus cerebros en maduración, a fin de maximizar cuánto tiempo pasan con sus plataformas y aumentar las ganancias.

(https://www.lavanguardia.com/vida/20230111/8674436/escuela-publica-seattle-demanda-redes-sociales-atacar-salud-mental-jovenes.html). Consultado el 12 de enero de 2023.

[46] Como el Código de buenas prácticas en materia de desinformación, entre cuyos firmantes estarán Google, Facebook, Twitter, Mozilla y asociaciones empresariales que representan al sector de la publicidad.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

se benefician de las conductas nocivas"[47]. Sus previsiones, incrementando las exigencias de transparencia y prohibiendo determinados comportamientos *online* se presentan como instrumentos idóneos para luchar contra el fenómeno de la desinformación. El establecimiento de obligaciones específicas para las plataformas en línea y especialmente aquellas de muy gran tamaño, así como la previsión de elevadas sanciones para las conductas más graves (artículo 52) y la garantía del derecho a presentar una reclamación de los destinatarios del servicio (artículo 53), contribuirán a proteger los derechos fundamentales de las personas en su actividad en las plataformas sociales, contribuyendo al sostenimiento de los valores democráticos. Por ello, el conjunto de medidas incluidas en el RSD para exigir a los prestadores de servicios que actúen de forma responsable y diligente para conseguir un entorno en línea seguro, predecible y que genere confianza, se deben valorar favorablemente.

No obstante, urge que el ordenamiento europeo se vea completado con la aprobación del Reglamento de IA, pues "una sola aplicación de Inteligencia Artificial puede impactar en una gran cantidad de derechos" (DE ASÍS ROIG, 2022: 102). Es necesario preservar adecuadamente los derechos de las personas que pudieran resultar afectados por los sistemas de alto riesgo y para, definitivamente, prohibir la puntuación o crédito social de las personas, los sistemas de IA que las clasifiquen a partir de sus datos biométricos en grupos por razón de su origen étnico, sexo, orientación política o sexual, así como la inferencia de emociones, que puedan dar lugar a la explotación de sus vulnerabilidades. Pues, como han señalado el SEPD y el CEPD, la IA ampliará la cantidad de predicciones que pueden hacerse, empezando por las correlaciones mensurables entre datos invisibles para los ojos humanos, pero visibles para las máquinas, lo que facilitara nuestras vidas y resolverá un gran número de problemas; pero, *"al mismo tiempo, erosionará nuestra capacidad de dar una interpretación causal a los resultados, de modo que los conceptos de transparencia, control humano, rendición de cuentas y responsabilidad por los resultados se verán seriamente cuestionados*"[48].

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

[48] Dictamen conjunto 5/2021 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), p. 6-7.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

Bibliografía

ALCARÁZ RAMOS, M. 2020. "Preguntas de la explosión tecnológica del conocimiento a la política democrática y al derecho", en FUENTES SORIANO, O. (Dir.). 2020. Era Digital, Sociedad y Derecho. 2020. Valencia: Tirant lo Blanch.

ALCOTT, H. y GENTZKOW, M. 2017, *"Social Media and Fake News in the 2016 Election"*, Journal of Economic Perspectives, vol. 31, nº 2.

AÑÓN ROIG, M. J. 2022. *"Desigualdades algorítmicas. Conductas de alto riesgo para los derechos humanos"*. Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos, nº 47, 2022.

BAKSHY, MESSING y ADAMIC. 2015. *"Exposure to ideologically diverse news and opinion on Facebook"*. Science, Junio de 2015, Vol. 348, nº 6239.

BARBU, BARBU, O. 2014. "Advertising, Microtargeting and Social Media", Procedia - Social and Behavioral Sciences 163.

BELLOSO MARTÍN, N. 2022. "La problemática de los sesgos algorítmicos (con especial referencia a los de género) ¿Hacia un derecho a la protección frente a los sesgos? En LLANO ALONSO, F. H. 2022. Inteligencia artificial y Filosofía del Derecho. Murcia: Laborum ediciones.

BELTRÁN PARDO, M y SEVILLANO JAÉN, F. 2013. Cloud computing, tecnología y negocio, Madrid: Paraninfo.

BENDER, E. M., GEBRU, T., MCMILLAN-MAJOR, A., & SHMITCHELL, S. 2021. On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, March 2021.

BYUNG-CHUL H. 2014. La sociedad de la transparencia. Barcelona: Herder, p. 109.

CAMPUZANO TOMÉ, Herminia: *Vida privada y datos personales. (Su protección jurídica frente a la sociedad de la información),* Tecnos, Madrid, 2002.

CARDON, D. 2018. Con qué sueñan los algoritmos: nuestras vidas en el tiempo de los Big Data. Madrid: Dado Ediciones.

COTINO HUESO, L. 2022. "Quién, cómo y qué regular (o no regular) frente a la desinformación". Teoría y Realidad Constitucional. n.º 49.

CC BY SA

DOI: https://doi.org/10.51915/ret.309

2023. "Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida". Revista Española de la Transparencia. Núm. 16. Primer semestre. Enero-junio de 2023.

CRAIG, T. y LUDLOFF, M. E. 2011. Privacy and Big Data, Sebastopol: O'Really, p. 6.

DE ASÍS ROIG, R. 2022. Derechos y tecnologías. Madrid: Dykinson.

ECHEVERRÍA, J. 2013. Entre cavernas. De Platón al cerebro pasando por Internet. Madrid: Triacastela.

GARCÍA MAHAMUT, R. 2015. *"Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español".* UNED. Teoría y Realidad Constitucional, núm. 35, 2015.

GARRIGA DOMÍNGUEZ, A. 2015. Nuevos retos para la protección de los datos personales. En la Era del Big Data y de la computación ubicua. Madrid: Dykinson.

2018. "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", en Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos, nº 38.

2021. "Decisiones automatizadas basadas en algoritmos y protección de datos personales", en Tomás Mallén, B., García Mahamut, R. y Pauner Chulvi, C. (Ed.): Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español. Cuestiones clave de orden nacional y europeo. Valencia: Tirant lo Blanch.

HOLIDAY, R. 2013. Confía e mi, estoy mintiendo. Confesiones de un manipulador de los medios. Barcelona: Empresa Activa.

IPPOLITA. 2012. En el acuario de Facebook. El irresistible ascenso del anarco-capitalismo. Madrid: En clave de libros.

KERR, I. y EARLE, J. 2013. "Prediction, preemption, presumption: how Big Data threatens big picture privacy", Stanford Law Review, Volume 66, num. 65.

KIRLEY E. 2016. *"The robot as cub reporter: law's emerging role in cognitive journalism"*, en European Journal of Law and Technology, Vol 7, No 3.

LANIER, J. 2018. Diez razones para borrar tus redes sociales de inmediato, Barcelona: Editorial Debate.

LORENZO CABRERA, S. 2018. "Posición jurídica de los intervinientes en el tratamiento de datos personales. Medidas de cumplimiento", en AA.VV.: Protección de datos, responsabilidad activa y técnicas de garantía. Madrid: REUS.

CC BY SA

LYON, D.2014. Surveillance Studies. An overview. Malden: Polity Press.

MAYER-SCHÖNBERGER, V. y CUKIER, K. 2013. Big Data. La revolución de los datos masivos. Madrid: Turner Noema.

O'NEIL, C. 2017. Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia. Madrid: Capitán Swing.

PARISIER, E. 2017. El filtro burbuja: Cómo la web decide lo que leemos y lo que pensamos. Madrid: Taurus.

PAUNER CHULVI, C. 2018. "noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red". UNED. Teoría y Realidad Constitucional, núm. 41, 2018.

RAMOS BERNAL, A. 2012. Reflexiones sobre economía cuántica, Alicante: ECU.

ROLLNERT LIERN. 2002. *"La libertad ideológica en la jurisprudencia del Tribunal Constitucional".* Cuadernos y Debates, nº 129. Madrid: Centro de Estudios Políticos y Constitucionales.

SAMUEL, A. L. 1983.First grade TEX: a beginner's TEX manual. Stanford Department of Computer Science.

SARIGOL, E., GARCÍA, D. y SCHWEITZER, F. 2014. "Online Privacy as a Collective Phenomenon", Proceedings of the second edition of the ACM conference on Online social networks, ACM, octubre de 2014. http://arxiv.org/pdf/1409.6197.pdf.

TENE, O. y POLONETSKY, J. 2012. "Privacy in the age of Big Data: a time for big decisions". Stanford Law Review Online, nº 63.

TOMÁS MALLÉN, B. 2015. *"Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales",* en RALLO LOMBARTE, A. y GARCÍA MAHAMUT, R. 2015. Hacia un nuevo Derecho europeo de protección de datos. Valencia: Tirant lo Blanch.

XIOL RÍOS, J. A. 2001. *"La libertad ideológica o libertad de conciencia"*, en AA. VV. 2001. La libertad ideológica. Actas e las VI Jornadas de la Asociación de Letrados del Tribunal Constitucional, Cuadernos y Debates n.º 115. Madrid: Centro de Estudios Políticos y Constitucionales.

ZUBOFF, S. 2019. La era del capitalismo de la vigilancia. Barcelona: Paidós.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Transparencia pública, genoma y datos genéticos

Jesús Jiménez López[1]
Director del Consejo de Transparencia y Protección de Datos de Andalucía
España

ORCID: 0009-0007-9421-9431

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

RESUMEN: Las actuaciones sobre el genoma, la información y los datos genéticos presentan riesgos para los derechos fundamentales, incluido el derecho a la protección de datos personales, y para la dignidad y libertad humana. En estas actuaciones destaca la intervención de las administraciones públicas, asi como de entidades e instituciones sujetas a las obligaciones de transparencia. Desde el punto de vista de las obligaciones de publicidad activa y del ejercicio del derecho de acceso a la información pública prevista en las Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, se concluye la necesidad de completar el espacio y el contenido de la transparencia necesaria, siendo objetivo de este trabajo la definición de un marco específico de cumplimiento. Para ello se identifican las singularidades de las actividades que tienen por objeto el genoma humano, la información genética y los datos genéticos en su contexto de uso legítimo, al objeto de definir un espacio específico de rendición de cuentas.

PALABRAS CLAVE: Transparencia, Información pública. Genoma. Datos Genéticos Personales. Derechos fundamentales, Dignidad y Libertad humana. Transparencia desde el diseño y por defecto.

[1] Director del Consejo de Transparencia y Protección de Datos de Andalucía. Letrado de la Junta de Andalucía (Exc.).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

CONTENIDOS: 1.-Introducción. 2.-Precisiones conceptuales. 3.-Singularidad de los datos genéticos. 4.-Derechos humanos, libertades fundamentales y respeto de la dignidad humana. *4.1.- Prohibiciones relativas a actuaciones relacionadas con el genoma. 4.2.-Limitaciones de finalidad en el tratamiento de datos genéticos. 4.2.1.-Diagnóstico y asistencia sanitaria. 4.2.2.- Investigación científica. 4.2.3.-Medicina forense y procedimientos civiles y penales u otras actuaciones legales. 4.3.-Autodeterminación. 4.4.-No discriminación y prohibición de estigmatización. 4.5.-Reparación de daño. 4.6.-Confidencialidad. Datos genéticos como datos personales.* 5.-Transparencia pública y genoma. *5.1.-Sobre la delimitación del espacio de transparencia. 5.2.-Sobre los sujetos obligados. 5.3.-Sobre la Publicidad activa. 5.4.-Sobre el ejercicio del derecho de acceso a la información pública.* 6.-Reflexión y propuesta final. -Bibliografía.

Transparency, genome and genetic data

ABSTRACT: Actions on the genome, genetic information and genetic data present risks to fundamental rights, including the right to the protection of personal data, and to human dignity and freedom. In these actions, the intervention of public administrations, as well as of entities and institutions subject to the transparency obligations stands out. From the perspective of the obligations of active publicity and the exercise of the right of access to public information provided for in Law 19/2013, of 9 December, about transparency, access to public information and good governance, the need to complete the space and the content of the necessary transparency is concluded. The aim of this paper is trying to offer a specific compliance framework. To this end, the peculiarities of the activities related to the human genome, genetic information and genetic data are identified in their context of legitimate use, in order to define a specific space of accountability.

KEYWORDS: Transparency, Public Information. Genome. Personal Genetic Data. Fundamental Rights, Dignity and Human Freedom. Transparency by design and by default.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

1.- Introducción

Las actividades realizadas desde el sector público sobre el genoma o sobre los datos genéticos, proporcionan innegables beneficios en los ciudadanos, vinculados con carácter general a la mejora en la salud de las personas, directamente en el marco de la asistencia sanitaria o como resultado de la investigación científica a su servicio. No obstante, estas actividades pueden tener impacto en la evolución de la especie humana, en los derechos fundamentales, y en el espacio de dignidad y libertad de las personas. Su alcance se incrementa a medida que avanzamos en el conocimiento científico, y su evolución presenta incertidumbres y riesgos ahora desconocidos.

Estas circunstancias han dado lugar a la definición de un marco de gobernanza específico, integrado por normas y principios construidos a partir de una identificación de los desafíos y dilemas éticos que la materia presenta, destacando en este punto un compromiso de prudencia, cautela y protección. En este marco destaca el principio de transparencia, no sólo necesario para hacer posible un debate que nos afecta a todos, sino también para exigir, a las personas y entidades que intervienen en este ámbito, una adecuada rendición de cuentas en el cumplimiento de las obligaciones que las citadas normas y principios les imponen. Debe considerarse parte de la garantía de su cumplimiento, posibilitando la exigencia de responsabilidades por los ciudadanos en este ámbito de la acción pública.

La actividad analizada tiene singularidades, como singularidades tiene la información y los datos a los que se refiere, especialmente sensibles. Así, se desenvuelve en un contexto de colaboración internacional, con múltiples protagonistas, con diferentes funciones, y competencias en el caso de los poderes públicos. Aun cuando se parte de un consenso sobre la transparencia, con normas y principios comunes, el marco estatal actualmente diseñado se revela insuficiente para darle cumplimiento.

Hablamos de genoma, información genética, de datos genéticos personales, y de transparencia en todas las actividades que les afectan. Esta precisión es necesaria pues no es objeto de estas palabras analizar el acceso a la información pública en su conflicto con la protección de los datos personales, aun de especial protección (Art. 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno [en adelante LTBG]). Tampoco hablaremos de la transparencia como principio de tratamiento de los datos personales[2]. Nos interesa en este momento la transparencia en la intervención sobre el genoma y en el tratamiento de los datos genéticos, de conformidad con la norma que regula

[2] Art. 5.1 RGPD, artículos 13 y 14 o 22 RGPD y concordantes LOPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

aquella, y su adecuación al marco de gobernanza en el que se integra. A este enfoque si responden, a modo de ejemplo, las obligaciones de publicidad activa referidas al Registro de Actividades de Tratamiento previstas en el artículo 6 bis LTBG.

En este documento inicialmente abordaremos las singularidades que presente el genoma, la información y los datos genéticos como objeto de intervención, en este caso desde el sector público. Esta es la base para definir un ámbito objetivo de transparencia necesaria. Advertidas las dificultades de asentar la rendición de cuentas en esta materia en la regulación contenida en la LTBG, sobre publicidad activa y ejercicio del derecho de acceso, se concluirá esbozando una propuesta.

2.- Precisiones conceptuales

No es este un tratado de genética, por lo que la inclusión de definiciones son meramente instrumentales al objeto de completar el supuesto de hecho o, al menos, las hipótesis que son consideradas en este breve estudio.

Desde este punto de vista consideraremos *genoma* la secuencia de nucleótidos que constituye el ADN de un individuo o de una especie[3] que se hayan en una célula, conteniendo toda la información genética que la persona necesita para desarrollarse y funcionar[4]. Por su parte, en cuanto analizamos la transparencia predicada también del tratamiento de los *datos genético*s, atenderemos a su definición contenida en el 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, -en adelante RGPD-), esto es, aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan información única sobre la fisiología o la salud de dicha persona física y que resultan, en particular, de un análisis cromosómico, del ADN o del ARN, o de cualquier otro elemento que permita obtener una información equivalente, de una muestra biológica de la persona física en cuestión (artículo 4.13 y Considerando 34 RGPD)[5].

[3] RAE, Voz "Genoma":

[4] ("Voz "Genoma" en Glosario de NATIONAL HUMAN GENOMA RESEARCH INSTITUTE", 2022, p. 1. Recuperado 2 de marzo de 2023 (https://www.genome.gov/es/genetics-glossary/Genoma).

[5] Los datos genéticos considerados pueden se tanto los iniciales, adquiridos durante el desarrollo prenatal, como los datos genéticos adquiridos durante la vida de la persona, resultado de las denominadas mutaciones somáticas. En este sentido Fundación PHG 2020 (p. 54). Interpreta la eliminación de la referencia "desarrollo prenatal" del borrador inicial de la propuesta normativa. En el mismo sentido la indicación "heredadas y adquiridas" en el Art. 4.13 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Esta aproximación nos permite una primera distinción entre el *dato genético* y la *muestra biológica de persona humana*, que contiene la información genética y que podemos definir como «cualquier material biológico de origen humano susceptible de conservación y que pueda albergar información sobre la dotación genética característica de una persona»[6].

La extracción de los datos genéticos a partir de la información genética de la muestra biológica se realiza mediante el *análisis o prueba genética*, entendido como el «procedimiento destinado a detectar la presencia, ausencia o variantes de uno o varios segmentos de material genético, lo cual incluye las pruebas indirectas para detectar un producto génico o un metabolito específico que sea indicativo ante todo de un cambio genético determinado»[7].

Íntimamente relacionado con el análisis o prueba genética se encuentra el denominado *cribado genético*, prueba genética sistemática realizada a gran escala, de una población o subconjunto, que tiene por objeto detectar rasgos genéticos en personas asintomáticas (art. 2. xiii) UNESCO 2003). Los cribados genéticos se integran en programas de salud pública[8] con el objeto de identificar determinantes genéticos, para los cuales una intervención médica precoz pudiera conducir a la eliminación o reducción de la mortalidad, morbilidad o discapacidades asociadas a tales determinantes (Art. 3.g) y 54 Ley 14/2007).

Debe precisarse que los análisis o pruebas genéticas pueden considerarse «tratamientos» desde el punto de vista del RGPD, si atendemos a la definición

[6] Art. 3.o) Ley 14/2007; en el mismo sentido el Artículo 2.i) de la Ley 11/2007, de 26 de noviembre, Reguladora del Consejo Genético, de protección de los derechos de las personas que se sometan a análisis genéticos y de los bancos de ADN humano en Andalucía y su desarrollo normativo (en adelante Ley andaluza 11/2007); y algo más completo el artículo 2.iv) de la a. Declaración Internacional de la UNESCO sobre datos genéticos humanos, de 16 de octubre de 2003 (en adelante UNESCO, 2003).

[7] Art. 3.a) Ley 14/2007 También pueden consultarse las definiciones contenidas en Art. 2.xii UNESCO 2003 y Art. 2.a) Ley andaluza 11/2007.

[8] Como programa de salud pública se encuentra sometido a un marco de gobernanza específico, pudiendo atenderse en este sentido a lo previsto en el Capítulo VIII, art. 19 del Protocolo Adicional Asistencia Sanitaria UNESCO; Documento «25 recomendaciones sobre las repercusiones éticas, jurídicas y sociales de los test genéticos» En adelante COMISIÓN EUROPEA, 2004, p. 13.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

contenida en su Art. 4.2), que incluye la «recogida, registro, extracción», sin perjuicio de los diversos tratamientos posteriores[9].

3.- Singularidad de los datos genéticos

Los datos genéticos de la persona presentan singularidades, ampliamente descritas, que justifican un marco específico de gobernanza, incluyendo obligaciones la transparencia. Podemos sintetizarlas del siguiente modo:

a. El carácter único de la información genética. La información genética permite distinguir a una persona de las demás. Ello es así porque cada persona posee una configuración genética característica, siendo por ello un elemento que posibilita su identificación[10].

No obstante, esta singularidad, no nos permite afirmar que la identidad de una persona se reduce a sus rasgos genéticos, pues en ella influyen múltiples y complejos factores, como los educativos, ambientales y personales, así como sus lazos afectivos, sociales, espirituales y culturales con otros seres humanos (Art. 3 UNESCO 2003). Por otro lado, el entorno natural y social de la persona, esto es, su estado de salud individual, sus condiciones de vida, su alimentación y su educación pueden dar lugar a mutaciones en el genoma[11].

b. La información genética puede revelar información científica, médica y personal tanto actual como futura de la persona. Nos referimos a información de salud, actual y futura – p.e. de personas en la actualidad asintomáticas, a partir de predisposiciones y predicciones-, y sobre su sexo, su origen racial o étnico[12].

Pueden contener información, conocimiento del estado de salud o predisposiciones, cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas. Esa capacidad predictiva puede ser mayor de lo que se supone en el momento de obtenerlos (ART. 4.a) iii) UNESCO 2003). Ello es así como consecuencia de la evolución en la disponibilidad y variedad de pruebas genéticas[13],

9 El Art. 3.w) de la Ley 14/2007, define como «tratamiento de datos genéticos de carácter personal» las «operaciones y procedimientos que permitan la obtención, conservación, utilización y cesión de datos genéticos de carácter personal». Esta misma norma también se refiere a tratamiento (Art. 1), cesión (Art. 5.2), acceso (art. 5.4 y 50), publicación (Art. 51) comunicación (art. 52) Conservación (Art. 52). UNESCO 2003, se refiere a recolección, obtención, extracción, tratamiento, interpretación, utilización, circulación transfronteriza, cruce y conservación. (Arts. 6.a), 9.a), 14, 15, 17, 18 y 22). La Ley andaluza 11/2007 a acceso (Art. 8), cesión (Art. 14), intercambio (Art. 27) conservación (art. 28).

10 Fundación PHG 2020 (p. 15).

11 Art. 3 a. de la Declaración Universal sobre el Genoma y los Derecho Humanos 53/152. Ratificada Asamblea General ONU 9/12/1998 (en adelante DUGDH).

12 GT 29. 2004, p. 4.

13 Párrafo AN, Parlamento Europeo, 2001.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

la capacidad tecnológica[14] y el incremento de operadores, y de fines, en el contexto del tratamiento de los datos genéticos, sobre todo en el ámbito de la investigación[15]. Esta singularidad se hace más evidente considerando que técnicamente pueden ser almacenadas durante largos periodos de tiempo[16].

c. La persona suele desconocer la información genética y ésta no depende de su voluntad individual[17].

d. Las pruebas genéticas pueden ofrecer información no solo del titular de la muestra, sino también de las personas integradas en su familia biológica –consanguíneos-, incluso fallecidas, o de generaciones futuras[18]. Puede incluso revelar información sobre la existencia o inexistencia de vínculos biológicos entre las personas, atribuidos, conocidos o desconocidos[19], y ello con independencia de cual fuese el objetivo real de dicha prueba. Eso supone que, respecto de un mismo resultado, se confronten derechos e intereses diversos que han de ser conciliados[20] como datos de *titularidad compartida*[21].

[14] Parlamento Europeo, 2001, p. 37; Fundación PHG 2020, p. 15: «Como se señaló anteriormente, las tecnologías genómicas se están utilizando para generar un mayor nivel de datos sobre la salud individual y la fisiología, para un número cada vez mayor de personas».

[15] GT 29, 2004, p. 5. También en el mismo sentido Fundación PHG 2020. «Como una gama cada vez más amplia de profesionales de la salud y la investigación están utilizando técnicas y datos genómicos, deben considerar si los datos que utilizan dan lugar a implicaciones para la protección de datos y, en caso afirmativo, cómo esto afecta su trabajo. En el futuro, el uso rutinario de estas tecnologías y la retención de los resultados de las pruebas dentro de los registros médicos electrónicos parece probable que aumente la escala y la naturaleza de la información que los profesionales de la salud y los proveedores de salud tendrán que tener en cuenta.» P. 15.

[16] "Esta característica de la información genómica puede entrar en conflicto con las obligaciones y principios discutidos en el capítulo 2 para minimizar, anonimizar o incluso eliminar datos en la medida de lo posible para proteger los derechos e intereses de las personas" (Fundación PHG 2020, p. 60).

[17] GT 29. 2004, p. 5.

[18] Apartado AN, Parlamento Europeo, 2001; GT 29, 2004 p. 5); Art. 4.a). ii) UNESCO, 2003.

[19] Memoria Protocolo Adicional al Convenio sobre Derechos Humanos y Biomedicina, relativo a las Pruebas Genéticas con Fines Sanitarios de 27 de noviembre de 2008 (en adelante Protocolo Adicional fines sanitarios Convenio Oviedo). Párrafo 130.

[20] Fundación PHG 2020, p. 82.

[21] Sancho López, 2021, p. 5.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

e. - Los datos genéticos pueden caracterizar a un grupo de personas (por ejemplo, comunidades étnicas)[22], pudiendo ser importantes desde el punto de vista cultural para las personas o los grupos (art. 4.a) iv) UNESCO 2003).

4.- Derechos humanos, libertades fundamentales y respeto de la dignidad humana

La actividad desplegada en torno al genoma, la recolección, el tratamiento, la utilización y la conservación de los datos genéticos humanos se observa siempre como una oportunidad para abordar graves problemas de la humanidad, vinculados a la salud de las personas y de sus grupos. No obstante, como se ha indicado, puede suponer riesgos para el ejercicio y la observancia de los derechos humanos y las libertades fundamentales y para el respeto de la dignidad humana[23]. No en vano, se ha considerado que el genoma y la información genética tiene *naturaleza tríptica* referida no solo a la persona y su entorno familiar, sino también a todos los seres integrados en la especie humana[24].

La información genética de la persona supone un riesgo para su libertad y dignidad en la medida en que estas se asientan en el reconocimiento del derecho al pleno desarrollo de su personalidad, a la total autodisponibilidad de sus posibilidades de actuación y a su autodeterminación[25]. Cualquier determinismo inherente al perfilado genético es un riesgo para la libertad de la persona, en la adopción de decisiones y en la elección de la forma en la que expone a la sociedad[26]. En sentido, como señala ALVAREZ GONZALEZ (2017. p. 26), la garantía de los derechos fundamentales se asienta en la capacidad de la persona de determinar el grado y alcance de la utilización de su información genética. La posibilidad de perfilado genético, y su utilización, se ha incrementado como consecuencia de una mayor capacidad tecnológica, en cuando a cantidad de datos tratados, no solo genéticos, respecto de los cuales se extraen inferencias, por los algoritmos empleados, en su caso integrando sistemas de inteligencia artificial, y por la capacidad de computación. El perfilado, la predicción de comportamientos, también sobre el estado y evolución de la salud de las personas, se anudan a consecuencias que necesariamente han de afectarles.

[22] GT 29, 2004, p. 5.

[23] UNESCO, 2003, p. 2.

[24] ALVAREZ GONZALEZ, S. 2007 (p. 43).

[25] El ser humano puede ser reducido a un mero objeto de la técnica (ALVAREZ GONZALEZ, S. 2007. p. 69).

[26] ALVAREZ GONZALEZ, S. 2007 (p. 67 y ss.).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Esta consideración puede adquirir más relevancia tras los avances en las técnicas de edición del genoma humano para tratar o prevenir enfermedades[27], configurándose un entorno en el que la diferencia de trato basada en el perfil genético de las personas en un riesgo cierto y actual.

Por tanto, en torno al genoma, los datos e información genética debemos responder a un dilema ético, cada vez más profundo y pertinente, en función de los avances en la materia y se revela la necesidad de una supervisión robusta en este ámbito[28] y la adecuada atención a los principios de transparencia y rendición de cuentas[29]. Por todo ello, se ha articulado un espacio ético de utilización del genoma y los datos genéticos, en el que insertan un conjunto de principios y normas. Podemos sintetizar las siguientes:

4.1.- Prohibiciones relativas a actuaciones relacionadas con el genoma

Se han establecido, con el adecuado consenso internacional, actuaciones prohibidas sobre el genoma, salvo aquellas que se encuentren debidamente justificadas por un interés superior:

a) Las intervenciones para editar, modificar el genoma humano sólo estarán justificadas cuando tengan por objeto proteger la salud de la persona[30], esto es, por

[27] «La edición del genoma humano tiene un gran potencial para mejorar la salud humana y la medicina. Las tecnologías de edición del genoma humano se pueden utilizar en células somáticas (no heredables); células de línea germinal (no para reproducción) y células germinales (para reproducción). Los beneficios potenciales de la edición del genoma humano incluyen nuevas estrategias para el diagnóstico, el tratamiento y la prevención de trastornos genéticos; nuevas vías para tratar la infertilidad; nuevas formas de promover la resistencia a las enfermedades; contribución al desarrollo de vacunas y mayor conocimiento de la biología humana» en documento «WHO Expert Advisory Committee on Developing Global Standards for Governance and Oversight of Human Genome Editing. Human Genome Editing: recommendations. World Health Organization, 2021 (en adelante Recomendaciones OMS 2021). P. 4.

[28] Recomendaciones OMS, 2001. P. 12.

[29] Partes 2 y 3 del documento «WHO Expert Advisory Committee on Developing Global Standards for Governance and Oversight of Human Genome Editing. Human genome editing: a framework for governance: World Health Organization; 2021 (en adelante Gobernanza OMS, 2021).

[30] "P. Considerando la existencia de un consenso internacional sobre las dos condiciones con arreglo a las que pueden desarrollarse la investigación y los cuidados genéticos humanos: - no deben permitirse terapias génicas en óvulos ni en espermatozoides (la línea germinal), ya que los efectos se transmitirían a las futuras generaciones. Se admitirán los cuidados aplicados exclusivamente a las células somáticas que actúan únicamente sobre el individuo; - debe permitirse la utilización de terapias únicamente para la curación de enfermedades, incluidas las enfermedades hereditarias, y no para influir en características que no constituyen un problema de salud1," (Parlamento Europeo, 2001, p. 11).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

razones de prevención, diagnóstico y terapéuticas[31], prohibiéndose la introducción de una modificación en el genoma de la descendencia[32].

b) Se prohíben expresamente las prácticas eugenésicas[33] y, en particular, las que tienen por finalidad la selección de las personas (Art. 3.2.b) CDFUE).

c) Se prohíbe expresamente la clonación reproductora de seres humanos[34], entendida como una intervención sobre el genoma que tenga como fin crear un ser humano genéticamente idéntico a otro ser humano vivo o muerto, por compartir la misma serie de genes nucleares[35].

d) Se prohíbe expresamente que el cuerpo humano o partes de este en cuanto tales se conviertan en objeto de lucro (art. 3.2.d) CDFUE y art. 7 Ley 14/2007).

---

31 Artículo 13 ("Intervenciones sobre el genoma humano") ([CONSEJO DE EUROPA, 1999, p.4); Art. 26.2.c) 10ª de la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida (en adelante Ley 14/2006)., considera infracción muy graves: «La selección del sexo o la manipulación genética con fines no terapéuticos o terapéuticos no autorizados».

32 "C) Son infracciones muy graves: a) La realización de cualquier intervención dirigida a la introducción de una modificación en el genoma de la descendencia." ([Ley 14/2007, de 3 de julio, de Investigación biomédica.", 2007, p. 36]).

33 RAE: Orientados al perfeccionamiento de la especie humana.

34 Art. 3.d) apartado 2 de la Carta de los Derechos Fundamentales de la Unión Europea. (2010/C 83/02)ES 30.3.2010 Diario Oficial de la Unión Europea C 83/389 (en adelante CDFUE). En el mismo sentido Art. 1.3 Ley 14/2006: «Se prohíbe la clonación en seres humanos con fines reproductivos». También en Parlamento Europeo, 2001: «Q. Considerando que no hay diferencia entre la clonación con fines terapéuticos y la clonación con fines reproductivos, y que cualquier relajación de la prohibición actual dará lugar a nuevos progresos en la producción y el uso de embriones…», «60. Reafirma por ello su posición de que la manera más eficaz y creíble de actuar contra la clonación de seres humanos es excluir tanto la llamada clonación terapéutica como la llamada clonación reproductiva de seres humanos; 62. Reafirma su exigencia de una prohibición, en lo posible a escala mundial, de la clonación de seres humanos…". Previamente el Parlamento Europeo cita su Resolución de 12 de marzo de 1997 en la que afirma que "ninguna sociedad puede justificar ni tolerar, en ninguna circunstancia, la clonación de seres humanos (...) ya que constituye una grave violación de los derechos humanos fundamentales, se opone al principio de igualdad de los seres humanos al permitir una selección eugenésica y racista de la especie humana, ofende la dignidad de la persona y requiere la experimentación con seres humanos».

35 Art. 1 del Protocolo Adicional al Convenio de Oviedo, por el que se prohíbe la clonación de seres humanos, de 12 de enero de 1998, ratificado el 7 de enero de 2000,

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

4.2.- Limitaciones de finalidad en el tratamiento de datos genéticos

El tratamiento de los datos genéticos debe justificarse precisamente por los riesgos que le son inherentes, inicialmente desde una perspectiva ética. Así, son finalidades legítimas en este tratamiento, exclusivamente[36]:

4.2.1.- Diagnóstico y asistencia sanitaria a las personas o grupos

Con carácter introductorio, los tratamientos de datos genéticos irán dirigidos a proporcionar un diagnóstico de enfermedad o proporcionar una comprensión de la progresión y el pronóstico de la enfermedad actual o futura[37], para su tratamiento, incluso antes de la aparición de los síntomas[38]. Así, se pretende incluso posibilitar una "*intervención médica precoz"* con el objeto de eliminar o reducir la mortalidad, morbilidad o discapacidades asociadas a los determinantes genéticos obtenidos[39]. En esta finalidad se incluiría el estudio, a partir de datos genéticos, de la reacción o respuesta a los medicamentos asociadas a los mismos, su metabolismo, permitiendo una terapia personalizada. Nos referimos a desarrollo de fármacos personalizados mejorando su respuesta terapéutica, en ahorro de sufrimiento y de efectos secundarios, tanto en el mismo desarrollo como en la fase de medicación[40].

Para la rendición de cuentas en este punto tiene especial importancia respetar un acceso no discriminatorio a las pruebas genéticas[41], garantizar su calidad y

[36] El art. 5 "finalidades" señala que "los datos genéticos humanos…podrán ser recolectados, tratados, utilizados y conservados solamente con los fines siguientes: …" Art. 5. UNESCO, 2003); Artículo 5 y siguientes RGPD.

[37] Fundación PHG 2020, p. 6. En el mismo sentido " (GT 29, 2004, p. 7, describe las pruebas genéticas de diagnóstico sirven para aclarar las causas de una enfermedad con manifiestos síntomas clínicos … y puede incluir también un componente de predicción con respecto a los familiares del interesado; y las pruebas genéticas predictivas para definir los cambios genéticos con muchas probabilidades de causar una enfermedad en una fase posterior de la vida de la persona que es objeto de las pruebas, con las incertidumbres inherentes).

[38] Parlamento Europeo, 2001, p. 58.

[39] Art. 3.g) y 54 Ley 14/2007.; en el mismo sentido Art. 2.l), art. 16 Ley andaluza 11/2007.

[40] Parlamento Europeo, 2001, párrafos 21 y 23; Parlamento Europeo, 2001, p. 67. También COMISIÓN EUROPEA 2004. párrafo 19; y Fundación PHG 2020, p. 10. También se habla de la la nutrigenómica (o genómica nutricional) es el estudio de la relación entre las variantes genómicas o la expresión génica, la ingesta de alimentos, los nutrientes y la nutrición, incluidas sus implicaciones para la salud. (Fundación PHG 2020, p. 10).

[41] En caso necesario, el acceso a los test genéticos debe ser rápido y realizarse con los recursos adecuados, sin discriminación por razón de género, origen étnico ni situación social y económica" (COMISIÓN EUROPEA, 2004, párrafos 12 y 16); Art. 45.a) Ley 14/2007.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

seguridad[42] – con una adecuada evaluación de riesgos-, respetando el principio de utilidad clínica de la prueba – individual o de grupo -[43].

Por último, desde el punto de vista del tratamiento de datos personales, en su consideración de datos especialmente protegidos, conforme al art. 9.1 RGPD, sería necesario para completar la base jurídica, salvar la prohibición de tratamiento mediante el consentimiento (art. 9.2.a); el cumplimiento de fines médicos (Art. 9.2.h); razones de Salud Pública (Art. 9.2.i) o los intereses vitales del interesado o de otra persona física (Art. 9.2.c) RGPD. Además, debemos acudir a la previsión contenida en el apartado 1 de la Disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD), amparando las bases jurídicas de tratamiento de datos personales contenidas en la Ley 14/2007, de 3 de julio, de Investigación Biomédica (en adelante Ley 14/2007).

4.2.2.- Investigación científica[44]

El tratamiento de datos genéticos humanos también puede justificarse en la investigación científica, siempre con el objetivo y orientación de resolver problemas

[42] La realización de pruebas genéticas, por su impacto en los derechos fundamentales, se considera una actividad sujeta a intervención administrativa. A modo de ejemplo art. 10 Ley andaluza 11/2007.

[43] Articulo 6 — Utilidad clínica. La utilidad clínica de una prueba genética será un criterio esencial para decidir ofrecer esta prueba a una persona o a un grupo de personas. (CONSEJO DE EUROPA, 1999, p. 3, protocolo adicional) 57. Por "utilidad clínica" se entiende el valor de los resultados de la prueba para orientar al interesado en sus elecciones de estrategias preventivas o terapéuticas. Por lo tanto, es un factor particularmente importante para decidir si es apropiado o no ofrecer una prueba genética. (CONSEJO DE EUROPA, 1999, p. 8) Explicación protocolo adicional. Por su parte el art. 9 («límites de los análisis genéticos») Ley 14/2007 señala: «2. 2. Los análisis genéticos se llevarán a cabo con criterios de pertinencia, calidad, equidad y accesibilidad. 3. Sólo podrán hacerse pruebas predictivas de enfermedades genéticas o que permitan identificar al sujeto como portador de un gen responsable de una enfermedad, o detectar una predisposición o una susceptibilidad genética a una enfermedad, con fines médicos o de investigación médica y con un asesoramiento genético, cuando esté indicado, o en el caso del estudio de las diferencias inter-individuales en la repuesta a los fármacos y las interacciones genético-ambientales o para el estudio de las bases moleculares de las enfermedades.». También de interés «VI.3. Pistas de reflexión para una intervención comunitaria con valor añadido… garantizar la igualdad de acceso a la información sobre la disponibilidad, el valor y las limitaciones de los análisis genéticos».

[44] Art. 5.ii) UNESCO 2003.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

de salud bien de las personas, bien de los grupos[45]. El tratamiento se justificaría conforme a las previsiones del Art. 9.2.j) RGPD ("tratamiento necesario para fines de investigación científica[46]") Art. 89.1 RGPD y la Disposición adicional decimoséptima LOPD.

En este sentido, por un lado claramente se afirma el sometimiento de las actividades de investigación científica al cumplimiento de normas y principios éticos, garantizado además mediante los *comités éticos,* como órganos colegiados que han de validar la investigación concreta propuesta[47]. Por otro, se parte del beneficio que aporta a la sociedad, imponiéndose a los poderes públicos la obligación de adoptar medidas que favorezcan la actividad investigadora[48] con garantía de calidad (Art. 5.d) DUGDH).

En este contexto adquieren relevancia los debates en torno a la disponibilidad de datos que sirvan de soporte a las investigaciones, y la anonimización como garantía para la protección de los datos personales, antes analizados. Así, destacan las previsiones en torno a la reutilización de los datos genéticos, las facilidades que ofrece la disposición adicional decimoséptima LOPD, en cuanto a las habilitaciones legales para el tratamiento, o las iniciativas enfocadas a proporcionar datos del genoma en el espacio europeo, pudiendo destacarse en este sentido la Declaración de Cooperación «Hacia el acceso a al menos 1 millón de genomas secuenciados en la Unión Europea para 2022» de 10 de abril de 2018[49], o la referencia al uso secundario de los datos genéticos contenida la propuesta de Reglamento de

[45] «Las aplicaciones de la investigación sobre el genoma humano, en particular en el campo de la biología, la genética y la medicina, deben orientarse a aliviar el sufrimiento y mejorar la salud del individuo y de toda la humanidad.» (Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997, ratificado el 13 de julio de 1999 (en adelante CONVENIO DE OVIEDO 1997).

[46] "…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".

[47] Art. 12 «Comités de Ética de la Investigación» Ley 14/2007; Disposición adicional decimoséptima, apartado 2.g) LOPD.

[48] Artículo 14 Los Estados tomarán las medidas apropiadas para favorecer las condiciones intelectuales y materiales propicias para el libre ejercicio de las actividades de investigación sobre el genoma humano y para tener en cuenta las consecuencias éticas, legales, sociales y económicas de dicha investigación, basándose en los principios establecidos en la presente Declaración." (CONVENIO DE OVIEDO 1997, p. 3).

[49] Declaración de Cooperación «Hacia el acceso a al menos 1 millón de genomas secuenciados en la Unión Europea para 2022» de 10 de abril de 2018. Disponible en: https://digital-strategy.ec.europa.eu/en/news/eu-countries-will-cooperate-linking-genomic-databases-across-borders. Consultado 17/4/2023.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Espacio Europeo de Datos Sanitarios[50]. Por último, destacamos la relevancia de los biobancos, como establecimientos que acogen muestras biológicas con fines diagnósticos y de investigación biomédica, organizada en torno a criterios de calidad, orden y destino (Art. 3. d) Ley 14/2007).

4.2.3.- Medicina forense y procedimientos civiles o penales u otras actuaciones legales[51]

En este caso debe encontrarse la habilitación final al tratamiento, bien en el consentimiento (art. 9.2.a) RGPD[52], bien en el interés público sustancial (Art. 9.2.g) y en las previsiones de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

[50] Art. 33.1.e) Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el Espacio Europeo de Datos Sanitarios. Estrasburgo, 3.5.2022 COM(2022) 197 final 2022/0140 (COD).

[51] Según en Art. 1.c) de la UNESCO 2003, sus disposiciones no se aplican a la recolección, tratamiento, utilización y conservación para la investigación, descubrimiento y el enjuiciamiento de delitos penales o de pruebas de determinación de parentesco, que se regirán por la legislación interna de los estados compatible con el derecho internacional relativo a los derechos humanos. Continúa diciendo su artículo 12, relativo a «Recolección de muestras biológicas con fines de medicina forense o como parte de procedimientos civiles o penales u otras actuaciones legales»: «Cuando se recolecten datos genéticos humanos o datos proteómicos humanos con fines de medicina forense o como parte de procedimientos civiles o penales u otras actuaciones legales, comprendidas las pruebas de determinación de parentesco, la extracción de muestras biológicas, in vivo o post mortem, sólo debería efectuarse de conformidad con el derecho interno, compatible con el derecho internacional relativo a los derechos humanos».

[52] Ver Art. 767, apartado 4, de la Ley de Enjuiciamiento Civil, sobre especialidades en materia de procedimiento y prueba, y la jurisprudencia sobre el precepto - por todas, Sentencia 299/2015, de 28 de mayo, del Tribunal Supremo, Sala de los Civil.-.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

4.3.- Autodeterminación[53]

Un elemento relevante en el cumplimiento de los principios y normas que garantizan la dignidad y libertad humana es el consentimiento[54] de la persona afectada, teniendo en cuenta su interés superior (Art. 5.b) CONVENIO DE OVIEDO 2007). De este modo, la recolección, tratamiento, utilización y conservación, como obligación impuesta por la ética[55], requiere previo consentimiento, libre[56], informado[57], expreso y escrito (Art. 4.1 y 48 Ley 14/2007), previéndose expresamente los supuestos en los que las personas afectadas no pueden emitirlo, su revocación[58], así como aquellos casos en los que la falta de consentimiento no puede ser un obstáculo al tratamiento[59]. Debe también considerarse desde la perspectiva del tratamiento de

[53] Principio 5 «autodeterminación», apartado a: «La prestación de servicios genéticos deberá basarse en el respeto al principio de la autodeterminación de las personas interesadas. Por este motivo, cualquier prueba genética, incluso cuando se ofrezca de manera sistemática, deberá estar sujeta al consentimiento expreso, libre e informado de la misma. b. Estará sujeta a especiales medidas de salvaguardia la realización de pruebas a las siguientes categorías de personas: — Menores de edad. — Personas que sufran trastornos mentales. — Adultos que se encuentren bajo tutela limitada. La realización de pruebas a dichas personas con fines de diagnóstico únicamente se permitirá cuando ello sea necesario para su propia salud o si la información fuese absolutamente necesaria para diagnosticar la existencia de una enfermedad genética en familiares. Será necesario el consentimiento de la persona que vaya a ser sometida a la prueba, salvo cuando la legislación nacional disponga otra cosa». Recomendación Nº. R (92) 3 del Comité de Ministros a los estados miembros Pruebas y exámenes genéticos con fines de atención médica, de 10 de febrero de 1992.

[54] Art. 3.f) Ley 14/2007 «Consentimiento»: manifestación de la voluntad libre y consciente válidamente emitida por una persona capaz, o por su representante autorizado, precedida de la información adecuada. No entramos en esta ocasión en el debate con relación a la distinción entre consentimiento informado desde el punto de vista de sujeto de atención sanitaria y el consentimiento conforme al RGPD. En este sentido, se ha considerado incluso una situación de desequilibrio dada la finalidad del consentimiento, desde el punto de vista de su libre emisión, desde la perspectiva del RGPD (Fundación GHP, p. 65); Art. 45.c) y d) Ley 14/2007.

[55] Art. 6.d) UNESCO, 2003. En el mismo sentido «recomendaciones sobre las repercusiones éticas, jurídicas y sociales de los test genéticos» COMISIÓN EUROPEA, 2004, apartado 23; y Parlamento Europeo, 2001, que expone el interrogante de como « garantizar el respeto de los valores, basados en la autonomía, esenciales en genética médica (consentimiento voluntario e informado, no existencia de presiones personales/sociales, promoción de la capacidad para tomar decisiones autónomas, prioridad de los derechos y los intereses individuales sobre los colectivos…», p. 72,

[56] GT 29, 2004, p. 7.

[57] Art. 6.d) y 11 ([UNESCO, 2003. También Protocolo Adicional Convenio de Oviedo Art. 8.

[58] Art. 9 UNESCO, 2003.

[59] Art. 17 UNESCO, 2003; Art. 9 Convenio de Oviedo, 1997.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

los datos genéticos posterior al que justificó inicialmente su emisión, estableciendo una adecuada ponderación entre los beneficios inherentes a la investigación, y las garantías en la protección de los datos personales[60].

Del mismo modo, también desde el punto de vista de autodeterminación, en este caso informativa, debe garantizarse el *derecho a saber* y a *no saber*[61], incluyéndose en este supuesto, el acceso a los propios datos genéticos[62]. Debe considerarse en este punto, como singularidad, su proyección sobre la familia biológica del interesado, sobre todo en aquellos supuestos en los que pueden surgir conflictos entre el derecho a no saber del afectado y el derecho a saber de sus consanguíneos. Dada la complejidad, incluso desde el punto de vista de dilema ético que puede plantearse, la cuestión debe resolverse en el caso concreto, mediante una ponderación de derechos e intereses en juego[63].

[60] Disposición adicional decimoséptima, apartados 2 y 3 LOPD.

[61] "El derecho a no saber: surge cuando la persona interesada elige no ser informada de los resultados de las pruebas genéticas, ni recibir otra información posteriormente (por ejemplo, sobre si es portadora de un gen defectuoso o si va a padecer una enfermedad), especialmente cuando la enfermedad es muy grave y no existe ningún medio científico de prevenirla o tratarla. Lo mismo sucede en el caso de los familiares que podrían hacer valer su derecho a no conocer los resultados de las pruebas practicadas a un miembro de su familia con el fin de determinar la presencia o ausencia de un desorden genético grave y preferirían vivir su vida sin la sombra de tal información. Esto es especialmente cierto cuando no existe ningún medio de prevención ni de tratamiento." GT 29, 2004, p. 10.

[62] Arts. 10 y 13 UNESCO 2003. El art. 5.c) del Convenio de Oviedo establece que: «Se debe respetar el derecho de toda persona a decidir que se le informe o no de los resultados de un examen genético y de sus consecuencias». En el mismo sentido Art. 49 Ley 14/2007. También Parlamento Europeo, 2001, p. 58 y GT 29, 2004, p. 10.

[63] Puede verse en este sentido GT 29, 2004, pp. 7 y ss. También Principio 11 de Recomendación N° R (92) 3 del Comité de Ministros a los estados miembros Pruebas y exámenes genéticos con fines de atención médica.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

4.4.- No discriminación[64] y prohibición de estigmatización[65]

Los principios y normas aplicables al tratamiento de datos genéticos impiden cualquier discriminación o estigmatización basadas en ellos. Con relación a la prohibición de estigmatización, son relevantes las conclusiones de los estudios de genética de poblaciones.

Esta prohibición de trato discriminatorio ha tenido especial importancia en el ámbito laboral y en el aseguratorio[66]. En el primer caso, para evitar que en la decisión de contratación o la determinación de las condiciones laborales tengan incidencia características genéticas de las personas, en particular cuando revelen una enfermedad o una predisposición genética - por otro lado basada en probabilidad-. También se puede considerar un espacio de riesgo de discriminación el ámbito de la contratación de seguros, pues las características genéticas, en su caso malinterpretadas o sobreestimada su importancia[67], podrían impedir el aseguramiento o tener impacto significativo en la determinación de las primas[68].

4.5.- Reparación de daño

Forma parte del marco ético el derecho a la reparación por los daños cuya causa directa y determinante haya sido la intervención en el genoma humano[69].

---

[64] Artículo 11. No discriminación. Se prohíbe toda forma de discriminación de una persona a causa de su patrimonio genético. Convenio de Oviedo 1997, siendo el principio enunciado en su art. 1; Artículo 7.a) «No discriminación y no estigmatización», UNESCO. 2003; Art. 6 DUGDH, según el cual «Nadie podrá ser objeto de discriminaciones fundadas en sus características genéticas, cuyo objeto o efecto sería atentar contra sus derechos y libertades fundamentales y el reconocimiento de su dignidad». Por su parte el Artículo 6 Ley 14/2007 «No discriminación» dispone: «Nadie será objeto de discriminación alguna a causa de sus características genéticas. Tampoco podrá discriminarse a una persona a causa de su negativa a someterse a un análisis genético o a prestar su consentimiento para participar en una investigación biomédica o a donar materiales biológicos, en particular en relación con la prestación médico-asistencial que le corresponda».

[65] Debemos entender por «estigmatización» como una calificación negativa de una persona o grupo debido a sus características, en este caso genéticas. Informe explicativo al Protocolo Adicional Convenio Oviedo, párrafo 58.

[66] "Se teme que las compañías de seguros y los empresarios puedan utilizar estos datos para denegar coberturas de seguros o puestos de trabajo. El acceso a esta información debe debatirse más para adoptar una normativa adecuada." (Parlamento Europeo, 2001, p. 59).

[67] JORQUI AZOFRA, M. 2017 (p. 108).

[68] GT 29, 2004, pp. 10 y 11.

[69] Artículo 8: «Toda persona tendrá derecho, de conformidad con el derecho internacional y el derecho nacional, a una reparación equitativa del daño de que haya sido víctima, cuya causa directa y determinante haya sido una intervención en su genoma.». DUGDH.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

4.6.- Confidencialidad. Datos genéticos como datos personales

Sin perjuicio de las singularidades que presentan, que justifica a nuestro juicio un marco de gobernanza pública y de rendición de cuentas específico, los datos genéticos se consideran con carácter general información sanitaria, y por tanto, incluidos en los datos de salud. Siendo cierto que los datos genéticos determinan características físicas, incluso étnicas, que por si los hacen acreedores de protección como datos especialmente protegidos[70], el régimen jurídico que aplica el RGPD no difiere de aquellos. En este sentido se ha descartado el denominado «excepcionalismo genético» que parte de una diferenciación de los datos genéticos de otro tipo de información sanitaria[71].

Señalado lo anterior, debemos considerar que la transparencia pública tiene entre sus límites la protección de datos personales. Por lo que es relevante delimitar el espacio de protección de los datos genéticos en el RGPD.

Para ello podemos distinguir:

- «Datos genéticos anónimos», esto es, registrados sin un nexo con una persona identificada o identificable (Art. 3.h) Ley 11/2007);

[70] Art. 9 RGPD. En este sentido se pronunció el Grupo de Trabajo Art. 29 en su Dictamen 3/2012, de 27 de abril, sobre evolución de tecnología biométricas señala: «Por ejemplo, los datos de ADN de una persona a menudo incluyen datos sobre la salud o pueden revelar el origen racial o étnico. En este caso, los datos de ADN son datos sensibles y deben aplicarse las garantías especiales previstas en el artículo 8, además de los principios generales de protección de datos de la Directiva». Por otro lado, no hay que olvidar el marco de protección de la confidencialidad que se extiende a las muestras biológicas se la que se extrae la información genética (Art. 53 y 70 Ley 14/2007 y Art. 4.b), UNESCO, 2003).

[71] "La información genética forma parte del espectro completo de información sanitaria y no constituye, como tal, una categoría aparte. Todos los datos médicos, incluidos los genéticos, merecen en todo momento los mismos niveles de calidad y confidencialidad." (COMISIÓN EUROPEA, 2004, apartado 3.p. 9); "A pesar de la incorporación explícita de «datos genéticos» por primera vez, el RGPD no marca la introducción del excepcionalismo genético en la ley de protección de datos de la UE. Esto se debe a que no existen derechos u obligaciones en el RGPD que se apliquen únicamente al tratamiento de «datos genéticos»; tres de las categorías especiales de datos «datos genéticos», «datos biométricos» y «datos relativos a la salud» siempre se toman en conjunto cuando se mencionan normas más específicas" (Fundación PHG 2020, p. 59).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

- «Datos anonimizados»[72], o "irreversiblemente disociados", por haberse destruido el nexo con toda la información que identifique al sujeto de la muestra, o la asociación exige un "esfuerzo no razonable"[73], mediante un proceso de anonimización[74];

- «Datos pseudonimizados», en los que se sustituye la información que identifica a la persona por un código, o información adicional, que permite la operación inversa[75];

- «Datos genéticos de carácter personal», con información que permite identificar a la persona a la que se refieren[76].

Son necesarias estas precisiones al objeto de evaluar el alcance de la inclusión de los datos genéticos en el ámbito de aplicación del RGPD, esto es, determinar cuando el *dato genético* es un *dato personal* en el sentido del reglamento. Desde este punto de vista podemos sin esfuerzo considerar que los datos pseudonimizados están sujetos al RGPD, al igual que la pseudonimización y anonimización, como tratamientos.

Si puede plantearse el debate en torno a los datos anónimos, bien por no haberse registrado el nexo con persona identificada o identificable, bien como resultado de un proceso de anonimización. En este sentido, y en primer lugar, se ha afirmado que los datos genéticos, como los datos biométricos, tienen una calidad dual pudiendo considerarse el contenido de la información sobre una persona y, además, el elemento para establecer un vínculo entre la información y una persona[77]. Esta calidad ha determinado un debate en torno a la identificabilidad intrínseca de los

[72] Art. 2.xi) UNESCO 2003; Art. 3.i) Ley 14/2007; Art. 2.g); Ley andaluza 11/2007.

[73] Entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados (Art. 3.i) Ley 14/2007.

[74] "…por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere". Art. 3.c) Ley 14/2001.

[75] Art. 4.5 RGPD; art. 2.x) UNESCO 2007; Art. 3.k) Ley 14/2007.

[76] Debe tenerse en cuenta en este sentido; art. 4.1 "datos personales" RGPD; Art. 2.ix UNESCO 2003); 3.j) Ley 14/2007; Art. 2.f) Ley andaluza 11/2007.

[77] "(L)a información puede identificar individuos, vincularlos con otros y revelar datos complejos sobre el futuro salud y desarrollo de esas personas y otras personas a las que están genéticamente relacionados" Opinión 6/2000 Grupo de Trabajo Art. 29. El Grupo de Trabajo también destacó: «Este carácter dual también se da en el caso de los datos sobre el ADN, que proporcionan información sobre el cuerpo humano y permiten la identificación inequívoca de una, y sólo una, persona» (Dictamen 4/2007 sobre el concepto de datos personales p. 9).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

datos genéticos[78] o incluso el alcance de la *individuación* respecto de la *identificabilidad*.

En segundo lugar, precisamente por el volumen y calidad de la información que los datos genéticos nos proporcionan, ahora y en el futuro, las herramientas tecnológicas, y el incremento de la información personal disponible, será cada vez más difícil una disociación irreversible de la persona de que se trate[79]. Esta reflexión debe ponerse en relación con el alcance la identificabilidad frente al denominado *intruso motivado*, considerado aquel con acceso a información, incluso pública, y la adecuada capacidad tecnológica[80]. En definitiva, se habla de dificultad e incluso imposibilidad de anonimización.

El principio de confidencialidad ha sido enunciado y regulado en todos los instrumentos internacionales y normas que regulan el tratamiento de los datos genéticos[81] y en las recomendaciones de las diferentes instituciones[82]. Se considera desde este punto de vista un requerimiento ético, articulado como garantía, y que ha sido matizado en relación con su uso para la investigación científica conforme al RGPD y LOPD.

5.- Transparencia pública y genoma

En los apartados anteriores hemos ido esbozando un esquema que nos delimita un marco básico para actuaciones que tengan por objeto el genoma humano, la información y los datos genéticos, tengan o no la consideración de datos personales a la luz del RGPD.

De la lectura de las singularidades que cualifican los tratamientos que tengan por objeto último el genoma humano y, en cualquier caso, el tratamiento de los datos

[78] «Esto se debe a que los datos genómicos pueden contener muchos marcadores que pueden ser referenciados, por ejemplo, con datos genéticos disponibles públicamente o porque pueden vincularse a signos y síntomas clínicos (información fenotípica) para identificar a un individuo. Sin embargo, es importante reconocer que esto no necesariamente hace que la información genética se identifique directa o intrínsecamente en sí misma» (Fundación PHG 2020, p. 40).

[79] UNESCO, 2003, p. 2. En tal sentido puede consultarse el informe publicado en MIT TECHNOLOGY REVIEW el 21 de enero de 2013 bajo el título "Un estudio revela problemas de privacidad en los datos del genoma". Disponible en: https://www.technologyreview.es//s/3264/un-estudio-revela-problemas-de-privacidad-en-los-datos-del-genoma. También Fundación PHG 2020, págs. 47 y ss.

[80] Fundación PHG 2020, p. 49.

[81] Art. 5, 45.b) y 51 Ley 14/2007; Art. 14 UNESCO, 2004; Arts. 7 y 9 Convenio de Oviedo 2007.

[82] Apartado 10. Recomendaciones COMISIÓN EUROPEA, 2004; principios 8 y 13 Recomendación Nº. R (92) 3 del Comité de Ministros a los estados miembros Pruebas y exámenes genéticos con fines de atención médica, de 10 de febrero de 1992,

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

genéticos, resulta, en un primer momento por su impacto en los derechos fundamentales, en la libertad y dignidad humana, la necesidad de garantizar el cumplimiento de un conjunto de obligaciones que deben asumir los poderes públicos, las administraciones públicas. Respecto de ellas debe asegurarse la rendición de cuentas[83]. Del mismo modo se revela necesidad de un debate general, también ético, en el que participen todos los implicados, la sociedad en su conjunto, incluidos los ciudadanos. Todo ello nos permite configurar un espacio de transparencia específico relativo a la acción pública desarrollada en torno a estas actividades.

Con ello no quiere decirse que exista un ámbito oscuro, oculto, en este marco de actuación de las Administraciones Públicas. Solo se pretende poner de manifiesto que la complejidad de la materia, y la dificultad para la compresión por la ciudadanía que ello supone, la multiplicidad de agentes que intervienen, dificultan su conocimiento público y su comprensión, debiendo plantearse si el marco normativo de transparencia actual (LTBG) es suficiente.

En este sentido, debemos considerar que la acción pública en esta materia se construye desde distintos ámbitos, ya sea en ejercicio de competencias normativas y ejecutivas, en la labor de supervisión, o incluso directamente en el tratamiento de datos genéticos en la asistencia sanitaria, la investigación científica o la realizada en el ámbito forense. En definitiva, su gobernanza tiene un marcado carácter transversal, en la medida en que en un mismo proyecto pueden participar, con distintas responsabilidades y cometidos, sujetos pertenecientes a distintas entidades, administraciones, incluso pertenecientes al sector privado, de distintos Estados, lo que contribuye a una segmentación que dificulta el conocimiento público ordenado y entendible. Se dificulta además la concreción de un marco jurídico que si bien se asienta en principios universales, no deja de ser disperso y en ocasiones confuso haciendo el esfuerzo de transparencia aún más necesario.

En definitiva, la transparencia se articula como elemento indispensable de gobernanza de la acción pública en el ámbito del genoma y en el tratamiento de datos genéticos y, como hemos indicado se enfrenta a diversas dificultades.

[83] En torno a ello, son varias las normas y recomendaciones que completan las previsiones de mecanismos de gobernanza específicos en materia de tratamiento de datos genéticos: Artículo 20. Dispositivo de supervisión y gestión, UNESCO, 2003; las Orientaciones la DUGDH, se refiere a la «organización de debates públicos sobre cuestiones de que trata la Declaración y el examen de los distintos procedimientos (conferencias con miras a lograr un consenso, consultas públicas, etc.» (Apartado 3.4.2); Documento «Human genome editing: a framework for governance». OMS, 2021.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Con el objeto de completar esta reflexión introductoria, merecen ser reproducidas las conclusiones de la OMS (Marco de Gobernanza OMS, 2021, párrafos 18 y 19)[84]:

«18. La buena gobernanza promueve la confianza del público velando por que las decisiones se tomen de manera transparente e inclusiva; e incluye medios para responsabilizar a los responsables políticos de esas opciones. Según sea necesario, la buena gobernanza también cuenta con mecanismos para hacer frente al incumplimiento de los mecanismos oficiales de gobernanza.

19. La buena gobernanza requiere acceso a recursos, capacidad y conocimientos técnicos adecuados para educar, involucrar y empoderar a los miembros de las comunidades científicas, médicas y de atención de la salud, así como al público. Por necesidad, los esfuerzos para educar, involucrar y empoderar incluirán esfuerzos para informar, escuchar, incorporar una gama de perspectivas y ser transparentes sobre quién es responsable de qué decisiones políticas, sobre la base de qué hechos, valores, principios y objetivos».

En este punto, con carácter general se expresa el preámbulo de la LTBG:

«La transparencia, el acceso a la información pública … deben ser … ejes fundamentales de toda acción política. Sólo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos y en términos similares».

[84] También mismo documento p. 24. Puede consultarse también Parlamento Europeo, 2021. Apartado 88, y apartado H: «.. y que estas ventajas sólo podrán aprovecharse plenamente si se permite un debate transparente e informativo y se ofrecen a los ciudadanos mayores facilidades para entender las posibilidades y los riesgos que entrañan los nuevos métodos». De importancia también; Recomendaciones 4 y 5 en «25 recomendaciones sobre las repercusiones éticas, jurídicas y sociales de los tests genéticos» COMISIÓN EUROPEA. 2004; Art, 6.a) UNESCO, 2003: «Por imperativo ético, deberán aplicarse procedimientos transparentes y éticamente aceptables para recolectar, tratar, utilizar y conservar los datos genéticos humanos y los datos proteómicos humanos. Los Estados deberían esforzarse por hacer participar a la sociedad en su conjunto en el proceso de adopción de decisiones referentes a políticas generales para la recolección, el tratamiento, la utilización y la conservación de los datos genéticos humanos y los datos proteómicos humanos y la evaluación de su gestión, en particular en el caso de estudios de genética de poblaciones. Este proceso de adopción de decisiones, que puede beneficiarse de la experiencia internacional, debería garantizar la libre expresión de puntos de vista diversos» y sus Arts. 20 y 24; Capítulo X «Debate Público», Convenio de Oviedo 1997; Capítulo IX «Información Pública» (Art. 20) Protocolo Adicional fines sanitario Convenio de Oviedo, 2008.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Veamos en qué términos puede darse cumplimiento a este mandato, sin ánimo de ser exhaustivo, más allá del enunciado de problemas generales[85].

5.1.- Sobre la delimitación del espacio de transparencia

Con carácter general, podemos aproximarnos a la transparencia necesaria, por un lado referida a la información relevante que permita el conocimiento del funcionamiento y el control de la actuación pública, entendida en el ámbito a que se refiere este estudio, respecto de la cual se exige publicación periódica y actualizada (Capítulo II "*Publicidad activa*" Art. 5 "*Principios Generales*", apartado 1 LTBG); y por otro, aquellos contenidos y documentos, cualquiera que sea su formato o soporte, que obren en poder de los sujetos obligados, con participación en el ámbito de estudio, y a los que todas las personas pueden acceder (art. 12 "Derecho de acceso a la información pública" LTBG).

Sobre la *publicidad activa* y sobre el objeto del ejercicio del *derecho de acceso a la información pública*, y sus dificultades en el ámbito de este escrito, nos referiremos a continuación. No obstante, en este apartado es conveniente hacer una delimitación inicial sobre cual consideramos que ha de ser su objeto, entendida como una concreción de la información necesaria para la exigencia de responsabilidades consustancial a la rendición de cuentas, o incluso para un adecuado debate ciudadano.

Como aproximación podemos considerar, a la vista de los apartados anteriores:

a) Identificación e información sobre agentes, Administraciones, Instituciones, entidades públicas y privadas, órganos que participan en actuaciones que supongan intervención sobre el genoma, o el tratamiento de información y datos genéticos, concretando sus roles, funciones y competencia.

b) Información sobre acciones o políticas públicas, de salud o investigación, relativas al genoma, la información y los datos genéticos, incluyendo propuestas normativas, estrategias, y cualquier otro documento de planificación, también presupuestaria. Recordemos en este punto el mandato de "formulación de políticas científicas públicas, asentadas en la ética, el rigor, prudencia, probidad intelectual e integridad, y teniendo siempre en cuenta sus consecuencias éticas, legales, sociales y económicas" ya comentado.

[85] No nos referiremos a la transparencia como principio de tratamiento de datos personales dada la acotación inicial (art. 13 y 14 RGPD y 15 RGPD).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

c) Procedimientos de gestión y supervisión para el cumplimiento de las normas y principios impuestos en la edición del genoma y el tratamiento de los datos genéticos[86].

d) Sobre los proyectos o actuaciones que supongan intervención en el genoma o el tratamiento de información o datos genéticos, toda la información necesaria para comprobar:

- El cumplimiento de las normas que prohíben determinadas finalidades o prácticas y la vinculación, en todo caso, a la protección de la salud de las personas;

- Que se realiza con las finalidades permitidas – diagnóstico y asistencia sanitaria, investigación científica, y medicina forense o entorno de procedimientos civiles, penales u otras actuaciones legales…-;

- La garantía de acceso no discriminatorio a las pruebas genéticas en el ámbito del diagnóstico y asistencia sanitaria, su calidad y seguridad, la adecuada evaluación de riesgos para la persona, y el respeto a los principios de utilidad clínica de las pruebas, ya sean individuales o de grupo;

- El cumplimiento de normas y principios éticos en la investigación que se refieran al genoma, la información y los datos genéticos, incluidos los procedimientos y la derivada de la participación de los Comités de Ética y otros órganos colegiados con similar cometido;

- El cumplimiento de normas y procedimientos para la protección de los derechos fundamentales, en particular las relativas al consentimiento, autodeterminación informativa, de las personas directa o indirectamente afectadas;

- La no discriminación y la prohibición de estigmatización basada en la información y datos genéticos, por ejemplo, como consecuencia de estudios de genética de poblaciones; el marco de reparación del daño causado, de forma directa o determinante, como consecuencia de la intervención en el genoma humano.

e) Información relativa al fomento de la actividad investigadora y su calidad, incluida la disponibilidad de información sobre el genoma, información y datos genéticos anónimos, en su caso en el contexto de espacios europeos de datos sanitarios.

f) Cumplimiento de normas que garanticen la confidencialidad de la información, así como el pleno cumplimiento de las normas de protección de los datos personales genéticos conforme al RGPD, siendo relevante en este sentido las medidas adoptadas para asegurar el carácter definitivo de la anonimización.

[86] Documento «Human genome editing: a framework for governance. » OMS, 2021, p. 47.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

No puede considerarse este marco de transparencia un espacio de acceso a la información como un derecho absoluto. Como hemos indicado, es necesario un ejercicio de ponderación entre el derecho de acceso a la información pública y la posible afección a los derechos e intereses privados (interesados, familiares, investigadores y centros, propiedad intelectual e industrial; e intereses públicos) con especial importancia de la protección de los datos personales.

Este puede considerarse un esbozo del espacio de rendición de cuentas a la que nos referimos, que puede completarse con la información pública vinculada las herramientas tecnológicas utilizadas, especialmente cuando por su complejidad se dificulta la comprensión y, en su caso, explicabilidad, ya sea frente a las personas que forman parte en el proceso de decisión, o frente a las personas interesadas o afectadas. Nos referimos, a modo de ejemplo, a las herramientas que incorporan sistemas o modelos de Inteligencia Artificial. Esta cuestión, compleja y espacio de riesgo en cualquier caso, no es objeto de este documento[87].

5.2.- Sobre los sujetos obligados

No se puede individualizar en una sola entidad o institución el cumplimiento de las obligaciones de transparencia sobre todas las políticas y actuaciones públicas que tengan por objeto el genoma, la información o los datos genéticos.

Hablamos de una materia en la que confluye la intervención de diversas instituciones y entidades, de sistemas públicos de salud y sus integrantes, de instituciones públicas con funciones de supervisión, control, inspección y sanción, entidades que articulan la intervención administrativa en el sector privado, instituciones de investigación, investigadores, laboratorios, etc.

Así, si quisiéramos enunciar una relación de sujetos obligados en este ámbito de acción pública, tendríamos en un primer momento los responsables de la adopción de decisiones articuladas a través de normas de carácter general y documentos de definición estratégica, incluidas las de carácter presupuestario (p.e. art. 2.1.a) LTBG). Tendríamos también los responsables del tratamiento del genoma, la información y los datos genéticos en el contexto de las finalidades autorizadas (p.e. art 2.1.a), c), d), e), g), h) e i) LTBG) entendiendo que en estas tipologías se incluyen tanto las que actúan en el ámbito de la investigación forense como quienes realizan actividades de asistencia sanitaria e investigación científica, íntimamente vinculadas. Podríamos completar esta enumeración no exhaustiva con los responsables de evaluar supervisar y garantizar el cumplimiento de las normas y principios aplicables en el sector público y en el sector privado (p.e. Art. 2.1.a) y c) LTBG). Hablamos, por tanto, no solo de Administraciones Públicas, sino también diversos agentes vinculados a

[87] Entre otra bibliografía puede consultarse COTINO HUESO, L. y CASTELLANOS CLARAMUNT, J, 2022. Sobre un estándar de transparencia algorítmica JIMENEZ LOPEZ, J. 2022. pp. 59 – 61.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

las asistencia sanitaria e investigación como profesionales sanitarios e investigadores del sector público, centros, promotores, Comités de Ética, Instituciones y órganos de autorización y evaluación de intervenciones, de difusión de las investigaciones y sus resultados, entidades de acreditación y autorización de centros de análisis y cribados genéticos, biobancos, el Registro Nacional de Biobancos, entidades de supervisión, inspección y de ejercicio de la potestad sancionadora, entre otros[88].

Cada una de estas entidades pueden tener un rol específico, competencia o función que afecta a la obtención, conservación y uso de muestras biológicas humanas, a la intervención en el genoma, la realización de análisis y cribados genéticos, y el tratamiento posterior de los datos genéticos, aún anónimos, con los fines autorizados indicados, en un mismo proceso complejo que determine o de lugar a los tratamientos. A partir de aquí, es donde pueden plantearse dificultades en torno a la realización efectiva del principio de transparencia, de la garantía del ejercicio del derecho de acceso, en los términos previstos.

No pretendemos analizar en este momento la naturaleza del derecho, que ha sido analizada por la doctrina más autorizada[89] sino poner de manifiesto que incluso el pleno cumplimiento de las obligaciones impuestas a los sujetos obligados por las normas contenidas en la LTBG, puede no ser satisfactoria para realización efectiva del principio de transparencia, en los términos que la materia demanda.

Si nos aproximamos a las obligaciones de publicidad activa, cuyo contenido analizaremos, se vinculan a los sujetos obligados individuales de forma concreta, que han de hacerlas efectivas en sus sedes electrónicas y páginas web (Art. 5.4 LTBG), siendo así que en este caso hablamos de actuación pública en la que participan diversos obligados.

A modo de ejemplo, desde la perspectiva de la protección de los datos personales, la dificultad de identificar a los responsables, corresponsables y encargados de tratamiento en un proyecto de investigación vinculada a la asistencia sanitaria, que suponga el tratamiento de datos genéticos personales, o que estos sean varios con distintos roles[90], necesariamente ha de afectar cumplimiento de las obligaciones de publicidad activa sobre los *registros de actividades de tratamiento* a que se refiere el artículo 6 bis LTBG, y, en cualquier caso, se corre el riesgo de que la información publicada por cada sujeto obligado esté segmentada dificultando la rendición de cuentas en el conjunto del proyecto.

[88] Todos ellos previstos, entre otras normas e instrumentos, en la Ley 13/2007.

[89] Entre otros GUICHOT y BARRERO pp. 66 y siguientes.

[90] Esta dificultad ha sido identificada en el tratamiento de datos genéticos (p.e. FUNDACION PHG. Pp. 32 y 33; LAGARZA 2019 pp. 24 y siguientes).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Lo mismo puede decirse sobre derecho de acceso, del que también hablaremos. Las participación de varios sujetos dificulta su ejercicio en la medida en que este ha de concretarse en el órgano administrativo o entidad que posea la información (Art. 17.1 LTBG) si bien cuando ha sido elaborada o generada en su integridad o parte principal por otro, se le remitirá para que decida sobre el acceso (art. 19.4 LTBG), y ello sin perjuicio del riesgo de inadmisión para el caso de no ser identificado correctamente el competente y desconocer su identidad (Art. 18.1.c) LTBG). Puede decirse que existe el riesgo de propiciar una peregrinación del ciudadano en la búsqueda de la información pública debilitando en cierta forma la rendición de cuentas que henos considerado cualificada en este ámbito.

En definitiva, la norma garantiza la transparencia de la actuación de un sujeto obligado pero se dificulta una transparencia real y efectiva en el caso de una actividad compleja en la que intervienen varios sujetos obligados, aun respondiendo del cumplimiento de normas y procedimientos comunes, con un marco de gobernanza específico. Recordemos que este marco se justifica en el riesgo que supone para los derechos fundamentales, y para la libertad y dignidad humana.

5.3.- Sobre la publicidad activa

Como hemos indicado, la publicidad activa supone exigir a los sujetos obligados hacer pública la información relevante de su actuación pública, permitiendo así el conocimiento del funcionamiento y su control (art. 5.1 LTBG). Como tal, habría de ser publicada en las correspondientes sedes electrónicas o páginas webs, de manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización. La información ofrecida forma comprensible, de acceso fácil y gratuito (arts. 5 y 11 LTBG).

En principio, estarían al servicio de la transparencia en un marco de gobernanza de la actividad de los poderes públicos respecto del genoma y los datos genéticos, las obligaciones de publicidad activa respecto de la organización y planificación (art. 6 LTBG) permitiendo el acceso a documentos de relevancia, en particular respecto de los denominados *comités de ética,* los *biobancos* o la planificación asociada a las políticas de salud pública mediante *cribados genéticos* de población y grupos. Más allá de la dificultad señalada por la participación de diversos sujetos obligados, la información difícilmente estará particularizada en los términos necesarios para hacer efectiva la rendición de cuentas en los ítems descritos en el apartado 6.1 de este documento.

Como obligación de publicidad activa, además de las descritas como Información de relevancia jurídica -que incluiría toda la actividad normativa en la materia en el contexto nacional- tendríamos que hacer referencia a la información económica, presupuestaria y estadística, vinculada a la acción pública sobre el genoma y al

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

tratamiento de datos genéticos (arts. 7 y 8 LTBG) de especial relevancia en el ámbito de contratos (art. 8.1.a) LTBG), convenios (art. 8.1.b) LTBG) y de subvenciones (art. 8.1.c) LTBG). De nuevo la información nos encontraríamos con información compartimentada, no atendiendo a nuestra finalidad específica.

De especial importancia en este ámbito, referido en concreto al tratamiento de datos genéticos personales, debemos considerar la exigencia de publicidad activa impuesta por el artículo 6 bis LTBG[91] sobre el *registro o inventario de actividades de tratamiento* y su contenido conforme al artículo 31 LOPD en relación con el artículo 30 RGPD, en la medida en que nos encontramos ante el tratamientos de datos especialmente protegidos y, en cualquier caso, su tratamiento entraña riesgo para los derechos y libertades de los interesados[92].

Esto supone someter a obligaciones de publicidad activa, la identificación de los responsables del tratamiento, y en su caso de los encargados de tratamiento, así como de los Delegados de Protección de Datos; las actividades de tratamiento llevadas a cabo; las finalidades de tratamiento; descripción de las categorías de interesados; descripción de las categorías de datos personales; las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas; los plazos previstos para la supresión de las diferentes categorías de datos; y la descripción general de las medidas técnicas y organizativas de seguridad (art. 32.1 RGPD).

Siendo cierto que este régimen de publicidad activa constituye un relevante instrumento de transparencia en los términos exigidos por las normas y principios antes indicados, lo cierto es que se enfrenta a algunas dificultades, con impacto directo en su utilidad, Así, las inquietudes suscitadas en torno a los riesgos para los derechos y libertades, la dignidad de las personas, resultan de la intervención de múltiples actores, con distintas funciones y responsabilidades, en distintos espacios –poderes públicos, comités de ética, investigadores, laboratorios, sistemas de salud- en un mismo ámbito. Por ello, el punto de conexión -«sujeto obligado»- atomizando la información, puede resultar insuficiente.

---

[91] "Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica. La referencia al artículo 77 supone una limitación en cuanto a los sujetos específicamente obligados," pues no incluye todos los contenidos en el Art. 3 LTBG, en concreto no incluye las Sociedades mercantiles Art. 2.g) LTBG.

[92] Artículo 9.1 RGPD es relación con el artículo 30.5 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Por último, no todas recomendaciones de publicidad específicas en el ámbito de las actuaciones sobre el genoma o de tratamientos de datos genéticos tendrían un encaje directo en estos supuestos de publicidad activa[93].

Así, es posible que diversas normas impongan obligaciones específicas de publicidad o difusión, o incluso prevean registros específicos para hacer públicos la existencia y resultados de los proyectos relativos al genoma, información y datos genéticos, Sin embargo, estas previsiones no pueden confundirse con el establecimiento de obligaciones de publicidad activa conforme a la LTBG. Es decir, estas obligaciones normativas están al servicio de las personas afectadas, por ejemplo, por ser quienes aportan las muestras biológicas, por ser los interesados en la información y los datos genéticos, o incluso a favor de toda la comunidad científica o asistencial, pero no están orientados a posibilitar el control por los ciudadanos de las actuaciones públicas, a los efectos de la rendición de cuentas, de exigencia de responsabilidades. Por ello, al no hablar de publicidad activa, de acuerdo con la LTBG, su eventual incumplimiento se rige por su norma específica, sin las garantías de la norma de transparencia, incluyendo, cuando proceda, la intervención de la autoridad de control conforme los arts. 23 y siguientes LTBG[94].

De este modo, el incumplimiento de estas obligaciones específicas, solo podrían determinar las reacciones jurídicas asociadas específicamente en la norma o aplicables, con las posibilidades impugnatorias que prevean en el ámbito administrativo o jurisdiccional. Todo lo anterior sin perjuicio del ejercicio del derecho de acceso a la información pública (art. 17 LTBG).

[93] A modo de ejemplo «I. NORMAS PARA UNA BUENA PRÁCTICA EN LA REALIZACIÓN DE PRUEBAS GENÉTICAS Y CRIBADO Principio 1. Información a la sociedad a. Los planes para la introducción de pruebas genéticas y cribado genético deberán darse a conocer a las personas, familias y a la sociedad. b. La sociedad deberá ser informada acerca de las pruebas genéticas y cribados, en especial de su disponibilidad, finalidad y consecuencias (médicas, jurídicas, sociales y éticas), así como en lo referente a los centros donde se realizan. …» Recomendación N° R (92) 3 del Comité de Ministros a los estados miembros Pruebas y exámenes genéticos con fines de atención médica, de 10 de febrero de 1992. También de interés «VI.3. Pistas de reflexión para una intervención comunitaria con valor añadido… garantizar la igualdad de acceso a la información sobre la disponibilidad, el valor y las limitaciones de los análisis genéticos».

[94] Pueden analizarse diversas resoluciones del CTPDA en este sentido, entre otras RESOLUCIÓN PA-79/2022, de 27 de octubre: "El Consejo únicamente podría tramitar las denuncias por estos incumplimientos en los supuestos en los que la normativa específica reconozca específicamente que la publicación tiene la consideración de obligación de publicidad activa, o bien pueda inferirse con claridad este carácter a la vista de la redacción de la norma".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

5.4.- Sobre el ejercicio del derecho de acceso a la información pública (arts. 12 y ss. LTBG)

En relación con el ejercicio del derecho de acceso a la información pública[95], partimos de su reconocimiento a todas las personas[96], considerando tal el derecho de acceso a «los contenidos y documentos, cualquiera que sea su formato y soporte, que obren en poder» del sector público y «que hayan sido elaborados o adquiridos en el ejercicio de sus funciones» (art. 13 LTBG). Como instrumento de transparencia, ya se han apuntado las dificultades que se nos presentan, en este ámbito, algunas comunes a otros espacios de la actuación pública.

Debemos recordar que el ejercicio del derecho de acceso a la información pública debe tener por objeto documentos existentes[97], de manera que debe tratarse de información cuya divulgación no requiera una acción previa de reelaboración (art. 18.1.c) LTBG), aún en su interpretación restrictiva enunciada por el Tribunal Supremo en su Sentencia 306/2020, de 3 de marzo[98].

Por otro lado, se revela el derecho de acceso como un instrumento insuficiente, en la medida que, al referirse a documentos existentes, su comprensión se asienta en su contenido, sin atención específica en este caso a su comprensión por un ciudadano medio.

También nos enfrentamos de nuevo a las dificultades asociadas a las singularidades de este ámbito de acción pública, con participación de diversos obligados en un mismo proyecto, en distintos ámbitos territoriales y con distintas funciones o competencias[99]. Esta circunstancia puede conducirnos, como hemos señalado, a una suerte de peregrinación que no solo consume tiempo, e incluso recursos públicos, sino que con frecuencia tiene resultados poco satisfactorios.

Por último, el ejercicio del derecho de acceso a la información pública, y su atención por los poderes públicos, se encuentran sujetos a una adecuada ponderación entre tal derecho y otros derecho e intereses de las personas que pudieran resultar

---

[95] No nos referiremos, dada la acotación inicial, a los límites del derecho de acceso (Art. 14 y 15 LTBG.

[96] Art. 105. b) CE, en relación con el Art. 12 LTBG.

[97] De importancia en este punto los Registros Públicos a que se refiere el apartado 76. Gobernanza OMS. 2021 y Apartado 1 Recomendaciones OMS 2021.

[98] "Ciertamente, el suministro de información pública, a quien ha ejercitado su derecho al acceso, puede comprender una cierta reelaboración, teniendo en cuenta los documentos o los datos existentes en el órgano administrativo. Ahora bien, este tipo de reelaboración básica o general, como es natural, no siempre integra, en cualquier caso, la causa de inadmisión prevista en el artículo 18.1.c) de la Ley 19/2013".

[99] Art. 18.1.d) y 2. Art. 19.4 LTBG.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

afectados, al igual que otros interese públicos (p.e. art. 14.1.e), g) y k) LTBG), conforme al art. 14.2 LTBG[100].

Sobre los derechos e intereses privados, desde este punto de vista, el derecho de acceso a la información pública relativa la actuación del sector público, particularmente en el ámbito de la asistencia sanitaria, pronóstico y atención, y de la investigación científica relacionada con ella, que tengan por objeto y afecte al genoma, o a la información y datos genéticos, puede enfrentarse a intereses económicos y comerciales, derechos de propiedad intelectual e industrial, o de protección de los datos personales (conforme al artículo 14.1.h) y j) y art. 15 LTBG en relación con el artículo 27 Ley 14/2007[101] y la disposición adicional segunda LOPD[102]).

Sin perjuicio de la necesidad de la ponderación, indispensable, la misma puede hacer necesaria la intervención de las personas titulares de los derechos o intereses afectados, en su garantía, mediante el trámite de audiencia al que se refiere el art. 19.3 LTBG, por un plazo de 15 días, con suspensión del plazo para resolver, trámite que también puede hacerse efectivo durante la tramitación de la eventual reclamación ante la autoridad de control en materia de transparencia, conforme al art. 24.3 LTBG. En cualquier caso, la oposición de las personas interesadas a posibilitar el acceso, impide su formalización inmediata a pesar de que pudiera ser concedido. Este acceso solo podrá tener lugar cuando "*haya transcurrido el plazo para interponer recurso contencioso administrativo sin que se haya formalizado o haya sido resuelto confirmando el derecho a recibir la información."* (Art. 22.2. LTBG).

No se cuestiona en este punto la previsión y esencia de la ponderación, más aún cuando la formulación de límites (art. 14 LTBG) y supuestos de inadmisión (Art. 18 LTBG) en el ejercicio del derecho de acceso, ha sido delimitado adecuadamente por la doctrina de las autoridades de garantía y control en materia de transparencia, y sobre todo por la jurisprudencia del Tribunal Supremo (ya enunciada en la Sentencia

[100] La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.

[101] Artículo 27. "Información sobre los resultados": "… 3. Los investigadores deberán hacer públicos los resultados generales de las investigaciones una vez concluidas, atendiendo a los requisitos relativos a los datos de carácter personal a los que se refiere el artículo 5.5 de esta Ley y sin menoscabo de los correspondientes derechos de propiedad intelectual e industrial que se pudieran derivar de la investigación."

[102] "La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

n.º 1547/2017, de 16 de octubre -Sala de lo Contencioso-Administrativo, Sección Tercera-) con un alcance restrictivo.

Lo que se quiere es poner de manifiesto es, por un lado, que en una materia tan compleja y con la confluencia de derechos e intereses públicos y privados, que han de ser analizados caso por caso, y que hacen complejo el ejercicio del derecho de acceso, no es el contexto más idóneo para una adecuada atención del principio de transparencia al servicio de la rendición de cuentas en este ámbito.

Por otro, si observamos detenidamente y atendemos a la práctica, es indudable que la formulación de límites, la configuración de su supuesto de hecho, se asienta en circunstancias sujetas a la previsión y control de los sujetos obligados. A modo de ejemplo, una adecuada política de gestión procedimental y documental de los proyectos, evitando supuestos de reelaboración, haciendo la documentación comprensible, adquiriendo o tutelando desde el inicio los derechos de propiedad intelectual o industrial, desarrollando políticas de pseudonimización y anonimización conforme al RGPD, permitirían la articulación de una *transparencia desde el diseño* y *transparencia por defecto*, al servicio, no solo del ejercicio del derecho de acceso a la información pública sino también a una publicidad activa ágil y eficaz. En cierta forma esta *transparencia desde el diseño y por defecto*, deben considerarse la otra cara de la moneda, respecto la Protección de datos personales desde el diseño y por defecto exigido en el RGPD.

6.- Reflexión y propuesta final

En este breve texto, considerando la complejidad de la materia abordada, se han puesto de manifiesto los beneficios que representan para las personas los avances en la asistencia sanitaria y en la investigación científica en el ámbito de la información genética y su tratamiento. Del mismo modo se ha abordado la respuesta dada al desafío ético que representa para la humanidad considerando el riesgo sobre los derechos fundamentales, el espacio de dignidad y libertad de las personas, de alcance final ahora desconocidos.

Su marco de gobernanza específico, esbozado, impone el principio de transparencia, como instrumento, no solo de un debate abierto en la sociedad, sino también como herramienta al servicio de la rendición de cuentas, al servicio de la exigencia de responsabilidades a los poderes públicos en el cumplimiento de sus obligaciones –impuestas precisamente como resultado de ese debate ético-.

La regulación contenida en la Ley 19/2013, se enfrenta a la realidad de los tratamientos de los datos genéticos, en el contexto de actividades y proyectos en los que intervienen múltiples actores, con distintas funciones y competencias, en distintos Estados o ámbitos territoriales.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Se propone, por tanto, por un lado, la *configuración legal de obligaciones específicas de publicidad activa*, con sometimiento expreso al marco de normas y principios previstas en la LTBG, incluyendo la garantía de intervención de la autoridad de control, en materia de transparencia. Del mismo modo, y en el mismo sentido, deben articularse estas obligaciones de publicidad activa en torno a un *punto único de acceso y publicidad* (sede electrónica específica, o página web), cualquiera que sea el origen de la información objeto de publicación, eligiéndose el modo adecuado de administración.

La información pública, referida al espacio de transparencia cuyo objeto ha sido delimitado en el *apartado 5.1*, deberá presentarse, publicarse, de manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización. La información ofrecida forma comprensible, de acceso fácil y gratuito. Dada la complejidad y relevancia de la materia, deberá ser presentada específicamente adaptada para su comprensión entendimiento en relación coherente con el cumplimiento de las pautas éticas definidas.

Al objeto de posibilitar el cumplimiento de estas obligaciones de publicidad activa, las políticas públicas, los procedimientos, la administración de los proyectos y las actuaciones sobre el genoma, la información y los datos genéticos deberán responder al principio de transparencia desde el diseño y por defecto, de acuerdo con una adecuada evaluación y en su caso corrección o presentación por capas, de las afecciones a derechos e intereses privados y públicos, incluida la protección de los datos personales, también desde el diseño y por defecto.

Esta propuesta esbozada no deja de ser un mero enunciado general, cuya concreción requerirá una atención más detallada a los problemas que sin duda presenta, acordes con el desafío que la intervención en el genoma, o sobre las informaciones y datos genéticos supone que para los derechos fundamentales, la libertad y dignidad de la persona.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia pública, genoma y datos genéticos
por Jesús Jiménez López
Págs. 165-198
DOI: https://doi.org/10.51915/ret.310

Bibliografía

ALVAREZ GONZÁLEZ, S. 2007. *Derechos fundamentales y protección de datos genéticos.* Madrid: DYKINSON

ALVAREZ GONZALEZ, S. 2017. "Derecho a la «privacidad» e información genética" en GARRIGA DOMINGUEZ, A. y ALVAREZ GONZALEZ. S. (Dirs.) 2017. *Un nuevo reto para los derechos fundamentales: los datos genéticos.* Madrid: DYKINSON

COLIN MITCHELL, JOHAN ORDISH, EMMA JOHNSON, TANYA BRIGDEN, Y ALLISON HALL. 2020. *El GDPR y los datos genómicos: el impacto del GDPR y la DPA 2018 en la atención médica genómica y la investigación*. Fundación PHG.

COTINO HUESO, L. y CASTELLANOS CLARAMUNT, J, 2022. Transparencia y explicabilidad de la inteligencia artificial. Valencia: Tirant lo Blanch

GUICHOT REINA, E y BARRERO DOMINGUEZ, C. 2020. El derecho de acceso a la información pública. Valencia: Tirant lo Blanch

JIMENEZ LOPEZ, J. 2022, "Oscuridad algorítmica en el sector público" en VESTRI, G. (Dir.) "La disrupción tecnológica en la administración pública: retos y desafíos de la inteligencia artificial. Cizur Menor: Thomson Reuters Aranzadi

JORQUI AZOFRA. M, 2017. "Implicaciones jurídicas de la obtención y utilización de resultados de pruebas predictivas (genéticas y no genéticas) en la contratación de seguros (I)" en GARRIGA DOMINGUEZ, A. y ALVAREZ GONZALEZ. S. (Dirs.) 2017. *Un nuevo reto para los derechos fundamentales: los datos genéticos.* Madrid: DYKINSON

RECUERO LINARES, M. 2019 "La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado". Trabajo realizado en el marco del Proyecto PMP17/00007 Functional and Clinical Impact of Genomic Analysis in CLL, integrado en el Plan Estatal de I+D+I y cofinanciado por el ISCIII-Subdirección General de Evaluación y el Fondo Europeo de Desarrollo Regional (FEDER - "Una manera de Hacer Europa").

SANCHO LÓPEZ, M. 2021. "Los "big data" genéticos y sus límites legales. Especial mención a la investigación con datos genéticos y la crisis del covid-19" *Revista Aranzadi de Derecho y Nuevas Tecnologías* 57/2021.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso?

David Díaz Lima[1]

Abogado especialista en protección de datos
Profesor de la Universidad Pontificia de Comillas
España

ORCID: 0009-0008-5657-1618

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

Este trabajo ha sido realizado en el marco del proyecto del Ministerio de Ciencia e Innovación DATATRANSCO con referencia n.º PID2021-128309NB-I00.

RESUMEN: Las Universidades tratan diariamente un volumen muy alto de información, propiciado por el uso de herramientas que colaboran a la digitalización de la información y a su utilización eficiente e inmediata. Esto representa una fuente de recursos que, utilizados de una forma eficaz, pueden favorecer la investigación científica, fomentar el crecimiento económico, la transparencia y, con ella, la participación ciudadana. Diseñar una Universidad transparente y comprometida debe hacerse no solo de modo teórico, sino llevándolo al terreno práctico, respetando los límites de acceso a la información que manejan y el respeto a la privacidad, para que genere utilidad y confianza en la sociedad a la que se revierten los servicios. La nueva Ley de Ordenación del Sistema Universitario español, si bien conlleva avances respecto a la ya derogada Ley Orgánica de Universidades del año 2001, se queda lejos de la concreción ya que la ejecución de las medidas se deja discrecionalmente en manos de las CCAA y/o de las Universidades. En protección de datos el retroceso es innegable ya que no existe ninguna referencia en la nueva normativa.

[1] Licenciado en derecho. Abogado especialista en protección de datos. Delegado de protección de datos en más de 100 entidades. Máster en Compliance. Autor de artículos en revistas y obras colectivas. Profesor Universitario en el doble Máster Universitario en Acceso a la Abogacía y Máster Universitario en Propiedad Intelectual, de la Universidad Pontificia Comillas ICAI- ICADE.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

PALABRAS CLAVE: Educación, Universidad, LOSU, Transparencia, Protección de datos personales.

CONTENIDOS: 1.-Introducción. 2.-Transparencia en el ámbito universitario. *2.1.-Marco normativo. 2.2.-La obligación de transparencia. 2.3.-El acceso a la información pública. 2.4.-La transparencia en la LOSU. 2.5.-Beneficios de la transparencia.* 3.-Protección de datos personales en el ámbito universitario. *3.1.-El tratamiento de datos personales. 3.2.-Proteccion de datos en la LOSU. 3.3.-Propuesta normativa.* 4.-¿Avance o retroceso en materia de transparencia y protección de datos en la LOSU? *4.1.-Reflexión en cuanto a los sujetos obligados, desde una doble óptica, LOSU y LTAIBG. 4.2.-¿Incompatibilidad entre transparencia y protección de datos? 4.3.-Desafíos de la transparencia en el ámbito universitario. 4.4.-Desafíos en el desarrollo de la protección de datos en el ámbito universitario*. - Bibliografía.

Transparency and protection of personal data in the university environment: progress or regression?

ABSTRACT: Universities deal with a very high volume of information on a daily basis, facilitated by the use of tools that contribute to the digitisation of information and its efficient and immediate use. This fact represents a source of resources that, if used effectively, may facilitate scientific research, promote economic growth, transparency and, thus, citizen participation. Designing a transparent and committed university must be done not only on paper, but also in practice, respecting the limits of access to the information they handle and respect for privacy, in order to generate usefulness and trust in the society to which the services are returned. Although the new Law for the Organization of the Spanish University System, brings with it advances with respect to the now repealed Organic Law on Universities of 2001, it falls far short of concreteness, since the implementation of the measures is left to the discretion of the Autonomous Regions and/or the universities. In the area of data protection, the backward step is undeniable, as there is no reference whatsoever in the new regulations.

KEYWORDS: Education, University, LOSU, Transparency, Personal Data Protection.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

1.- Introducción

La transparencia se ha convertido hoy en día en una demanda incuestionable por parte de los ciudadanos para todas las Administraciones, y entre ellas, la Universidad, donde se presume que los principios éticos deben ser una constante en su organización y funcionamiento.

La transparencia es un principio fundamental en una sociedad democrática y se considera un elemento clave para fomentar la rendición de cuentas y la confianza en las instituciones públicas, así lo reconoce nuestro texto constitucional en su art. 103.1 CE cuando indica que "la Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho"; pero también podemos derivar su exigencia del art. 20.1.d) CE cuando se reconoce y protege el derecho "A comunicar o recibir libremente información veraz por cualquier medio de difusión", y del artículo 105.1.b) CE cuando indica que la Ley regulará "El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

En el ámbito universitario, la transparencia es especialmente importante debido a la relevancia que tienen las universidades en la formación de ciudadanos y en la generación de conocimiento, tal y como señala la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (en adelante LOSU)[2].

En los últimos años hemos asistido a cambios, por un lado, en el terreno tecnológico y, por otro lado, un cambio en la mentalidad de los ciudadanos, que cada vez son más conscientes del valor de la información pública, pero también de la importancia de su información personal y demandan mayor conocimiento de lo que hacen los poderes públicos, y de lo que los mismos hacen con sus datos personales.

Las Universidades deben ser y dar ejemplo de transparencia, deben formar a sus estudiantes en una cultura de la transparencia, de respeto a los derechos fundamentales. De ahí la importancia de encontrar un equilibrio en este terreno entre la obligación de transparencia y la también obligación de proteger la información personal de los miembros de la comunidad universitaria.

Por un lado, los avances tecnológicos y los servicios que ofrecen permiten a las Universidades recoger, almacenar, intercambiar y suministrar enormes cantidades de información (entre ella, información personal), además de favorecer la relación

[2] Ley orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU) (BOE de 10 de diciembre de 2013). Vid. Preámbulo, arts. 2.2.a) y h) y 12 LOSU.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

entre los distintos miembros que componen la comunidad universitaria. Así, por ejemplo, se facilita la relación entre profesores y estudiantes a través del correo electrónico institucional o a través de plataformas virtuales institucionalizadas, o se manejan e intercambian numerosos datos en los procesos de matriculación, calificación o muchísimas otras actividades de gestión académica (Troncoso, 2006, 82-83; y 2017). Es evidente que las Universidades siempre han tratado datos personales, de sus estudiantes o de sus trabajadores, ya sea profesorado o personal de administración y servicios y con la finalidad de cumplir con una actividad administrativa, con una misión o en interés público, pero paulatinamente este tipo de información se ha ido multiplicando y su tratamiento se ha ido modernizando.

Por otro lado, la exigencia de transparencia, especialmente desde la aprobación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno ha obligado a las Universidades (en adelante, LTAIBG)[3], así como al resto de sujetos obligados por el artículo 2 de esta Ley, a tener un funcionamiento alejado de la opacidad porque, como queda reflejado en su Preámbulo:

"sólo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones, podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos".

Si la idea es que la Universidad contribuya a una cultura de la transparencia, debe predicar con el ejemplo.

Este ejemplo se lleva a la práctica con los valores que representa el Gobierno abierto[4], enfoque que promueve la transparencia, la participación ciudadana y la rendición de cuentas en la gestión pública, buscando fortalecer la democracia y mejorar la calidad de la gestión pública. Se basa en la idea de que el Gobierno debe ser accesible y receptivo a los ciudadanos, fomentando la colaboración y la apertura en la toma de decisiones y en la gestión de los asuntos públicos, y ello implica la adopción de medidas y políticas que buscan fortalecer la confianza y la legitimidad de las instituciones públicas (Arenas, 2016, 113-131; y Arenas, 2020, 107-134).

[3] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIB) (BOE de 10 de diciembre de 2013).

[4] Sobre estos principios y valores, vid. OECD, Recommendation of the Council on Open Government – OECD, 14 de diciembre de 2017. - C(2017)140 - C/M(2017)22. Paris: OECD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

Algunas de las características principales del Gobierno abierto incluyen:

En primer lugar y de forma esencial, la transparencia: Se refiere a la divulgación de información relevante sobre las actividades y decisiones del Gobierno. Esto implica proporcionar acceso a la información de manera clara, comprensible y oportuna, permitiendo a los ciudadanos conocer y evaluar las acciones del Gobierno.

En segundo lugar, se hace indispensable hablar de la participación ciudadana: Implica la inclusión de la ciudadanía en los procesos de toma de decisiones y en la formulación de políticas públicas. Se busca garantizar la participación efectiva de los ciudadanos, a través de consultas públicas, audiencias, mecanismos de retroalimentación y otras formas de involucramiento.

En conexión con la participación, se requiere que exista una colaboración: Fomenta la cooperación entre el Gobierno y la sociedad civil, así como la colaboración entre diferentes actores públicos y privados. Se busca establecer alianzas y acuerdos que permitan abordar problemas complejos y encontrar soluciones conjuntas.

Y, por último, no se puede hablar de transparencia sin hablar de rendición de cuentas: Se refiere a la obligación de los funcionarios y las instituciones gubernamentales de dar cuenta de sus acciones y decisiones. Esto implica establecer mecanismos de supervisión y control, así como procesos claros para investigar y sancionar la corrupción o el abuso de poder.

Pues bien, estos valores que el Gobierno abierto representa[5], deben formar parte igualmente del ámbito universitario porque con ellos se busca se busca reducir la opacidad y la mala praxis en la Universidad. No obstante, buscar el punto de equilibrio, como hemos señalado, para diseñar el modelo de Universidad transparente que queremos, debe hacerse desde el respeto a la privacidad, generando confianza en los ciudadanos a los que sus servicios van dirigidos.

2.- Transparencia en el ámbito universitario

2.1.- Marco normativo

El 22 de marzo de 2023 se publicó la citada Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU)[6], que entró en vigor a los 20 días desde su

[5] Recordamos aquí que sobre estos principios y valores, vid. OECD, Recommendation of the Council on Open Government – OECD, 14 de diciembre de 2017. - C(2017)140 - C/M(2017)22. Paris: OECD.

[6] Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

publicación, y que ha venido a sustituir a la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades[7], modificada por la Ley Orgánica 4/2007, de 12 de abril[8].

En primer lugar vamos a ver la obligación de transparencia y el acceso a la información pública junto a sus ventajas para, en el último apartado de este artículo, tratar de llegar a una conclusión sobre si estamos ante un avance o un retroceso tanto en la transparencia en el ámbito universitario como en la protección de datos como límite coherente a este derecho.

2.2.- La obligación de transparencia

La transparencia, como ya hemos indicado, se refiere a la obligación que tienen las instituciones públicas de poner a disposición de la ciudadanía información relevante y de interés general y de darles acceso a la misma, por eso podemos hablar de una publicidad activa (publicar) y una publicidad pasiva (acceso a la información) (Palomares Herrera, 2022; y Pérez Conchillo, 2023)[9]. Esta información debe ser accesible y comprensible, permitiendo que los ciudadanos puedan conocer cómo se toman las decisiones y cómo se utiliza el dinero público.

La transparencia, en el caso de las universidades, se refiere a la obligación de proporcionar información clara y accesible a la comunidad universitaria y a la sociedad en general. Esto implica una serie de prácticas y políticas que aseguran que la información relevante esté disponible, como los resultados de sus investigaciones, sus planes de estudio, los criterios de admisión y evaluación de los estudiantes, y los presupuestos y gastos de la institución y se comunique de manera efectiva a través de diversos canales, como sitios web, informes, boletines informativos, reuniones y consultas[10].

La transparencia implica que los ciudadanos deben tener acceso a la información pública de una forma rápida y detallada, pero ¿qué debemos entender por información pública? Más allá de la definición que ofrece la LTAIBG en su art. 13, según el profesor Piñar Mañas, reproduciendo lo que dice la citada Ley, por información pública se entiende que son "los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones" (Piñar, 2014, 10-11). Los ciudadanos exigen estar

[7] Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (LOU).

[8] Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

[9] Arts. 5-11 y 12 a 24 LTAIBG, respectivamente.

[10] Todo ello forma parte de las obligaciones de transparencia tanto activa como pasiva, o derecho de acceso, que las impone la LTAIBG.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

informados y participar en mayor medida en el proceso de todas de decisiones que les afecten (Lizcano, 2012-2013, 161).

En la actualidad, la aproximación que se hace a la transparencia, como uno de los principios asociados a la rendición de cuentas y a la gobernanza en las organizaciones públicas, ya no centra el debate solo en la difusión activa de la información, sino en la insuficiencia que pueda existir de disponibilidad y acceso a grandes volúmenes de datos, lo que trae consigo la rendición de cuentas (vid. García Muñoz, Arias Rodríguez, Chaves García, e Isabel Caro, 2023, 99-232)[11] y la gobernanza del conjunto de instituciones públicas, incluyendo las universidades, unas instituciones que, no solo han sido testigos del auge del movimiento social en favor de la transparencia, sino en el conjunto de medidas legales destinadas para tal fin (en nuestro caso, en España), a pesar del aumento del uso del "secreto institucional" como medida de restricción del acceso a datos, por motivos de seguridad nacional o protección de otros derechos (ej. derecho a la intimidad o protección de datos personales).

Hemos hecho referencia a las Universidades públicas, como entidades obligadas del art. 2.1.d) LTAIBG, pero esta exigencia debería pesar también sobre las Universidades privadas en la medida de que su finalidad no difiere del propósito esencial de las Universidades públicas, esto es formar y transmitir conocimiento a la sociedad. Así lo expresó el Consejo para la Transparencia y Buen Gobierno (CTBG) en su Criterio Interpretativo C/0003/2015[12].

2.3.- El acceso a la información pública

La citada LTAIBG establece, en su artículo 12, que "Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley", y lo desarrolla estableciendo su ejercicio y sus límites, completando así lo también dispuesto al respecto tanto por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector

[11] Los autores defienden la necesidad de transparencia en el terreno de los proyectos de investigación, donde hay implicados fondos públicos y la opacidad suele ser la regla.

[12] Vid. Criterio Interpretativo C/0003/2015, del Consejo para la Transparencia y Buen Gobierno.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

Público, especialmente en sus arts. 3.1,b)[13] y 81.1[14], como por la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones públicas (en adelante, LPACAP).

Para un ejercicio verdadero de transparencia al derecho de acceso se deben sumar unos adecuados mecanismos de control que hagan efectiva la rendición de cuentas. La rendición de cuentas no consiste sólo en ofrecer cifras o información de las actividades llevadas a cabo, sino que debe llevar aparejada la responsabilidad correspondiente ante las anomalías detectadas (Villoria, 2014-2015, 99-100; y Casares, 2018). La mera información de datos y resultados sin un mecanismo de control puede producir todo tipo de disfuncionalidades como el manipular la información u ofrecerla sesgada (Zapico, 2013, 331-356). De ahí que en el control también se hace necesaria una participación ciudadana y su colaboración. A ello contribuyen y pueden contribuir en gran medida los avances tecnológicos, pues las Administraciones públicas dejan de esperar a que el ciudadano les solicite información, para ofrecerla ellas de forma autónoma. Esto es, se pasa de un modelo "reactivo" a un modelo "proactivo", que los ciudadanos sabrán agradecer y que ofrece ese valor añadido del que ya hemos hablado (García, 2014, 78-79).

En el ámbito universitario el derecho de acceso a la información pública es una herramienta para hacer efectiva la obligación de transparencia que pesa sobre las Universidades. No obstante, en los años que lleva vigente la Ley de Transparencia española, la obligación de transparencia se ha centrado más en una transparencia activa, y las cuestiones que se han suscitado relacionadas con el derecho de acceso han sido las relativas a consultas sobre los salarios de los integrantes de órganos de gobierno universitarios, así como las referentes a las demandas de privacidad frente a la transparencia de los sujetos implicados y no está siendo realizada de forma efectiva (Barstow y Johnson, 2016)..

Para resolver muchos de los conflictos surgidos, desde la Conferencia de Rectores de las Universidades Españolas (CRUE) se publicó en julio de 2019 la Guía de buenas

[13] Artículo 3 Ley 40/2015 donde se recogen los. Principios generales: "1. Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho. Deberán respetar en su actuación y relaciones los siguientes principios: c) Participación, objetividad y transparencia de la actuación administrativa".

[14] Artículo 81 Ley 40/2015, donde regulando los principios generales de actuación señala: "1. Las entidades que integran el sector público institucional están sometidas en su actuación a los principios de legalidad, eficiencia, estabilidad presupuestaria y sostenibilidad financiera así como al principio de transparencia en su gestión. En particular se sujetarán en materia de personal, incluido el laboral, a las limitaciones previstas en la normativa presupuestaria y en las previsiones anuales de los presupuestos generales".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

prácticas en materia de transparencia y protección de datos personales[15], recogiendo los pronunciamientos más destacados sobre la materia de los órganos de garantía tanto de transparencia como de protección de datos. Así, en relación con el ejercicio de los derechos de acceso encontramos numerosos ejemplos. Entre otros cabe mencionar el acceso a datos académicos, acceso al contenido de trabajos fin de grado (TFG) o fin de máster (TFM), publicación de los listados con las calificaciones de los estudiantes, datos de contacto referidos al puesto, acceso a material científico, acceso a información relativa a proyectos de investigación, acceso a datos retributivos, acceso a documentación de órganos colegiados, acceso a los currículos de los miembros del equipo de gobierno, entre muchos otros (Troncoso, 2017).

2.4.- La transparencia en la LOSU

En la nueva Ley Orgánica del Sistema Universitario (LOSU) se ha avanzado en cuanto a la profusión de artículos donde aparecen referencias explícitas a la transparencia. Específicamente podemos encontrar las referencias en el Preámbulo, de transparencia editorial; transparencia en la conferencia de política universitaria (art.15); gobernanza (art. 44); transparencia financiera (art. 59); gestión del conocimiento (arts. 11 a 13, 18, 23, 39, 56, y 61); fundaciones públicas (art. 63); acreditación de cuerpos docentes (art. 69); concursos de acceso a plazas docentes (art.71); transparencia retributiva del personal técnico y administrativo (art. 93); carrera profesional (arts. 69 y 90); acceso del personal técnico (art.91); provisión de puestos de trabajo (art. 92); retribuciones (art. 93); régimen económico y financiero (art. 100).

Igualmente hay referencias indirectas como cuando se menciona la obligación de publicar, por ejemplo, los resultados de los proyectos de investigación (arts. 13 y 62)

Haciendo un análisis más pormenorizado de lo establecido en la LOSU, nos gustaría destacar los puntos que consideramos más relevantes:

- La ley establece que se debe garantizar el derecho de acceso a la información que se consideren institucionalmente relevante (art. 39).

- Las instituciones universitarias deben realizar una publicidad activa de la información relevante (arts.31, 33, 69, 86, 91, 92, 93, Disposición transitoria séptima y Disposición transitoria novena).

- Las instituciones universitarias deben rendir cuentas sobre su gestión y sobre el uso de los recursos públicos presentando informes periódicos detallados sobre el

[15] Vid. CRUE. 2019. Guía de buenas prácticas en materia de transparencia y protección de datos personales.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

uso de los recursos, resultados y medidas adoptadas para mejorar la gestión (arts.53 a 63)

- La participación ciudadana es fundamental para garantizar la transparencia en las instituciones universitarias, para ello se deben promover mecanismos de participación como los consejos sociales (art.47).

- Transparencia en la gestión de la investigación. Publicación de los resultados de la investigación y la divulgación de los métodos utilizados para obtener dichos resultados (arts.11, 13 y 39).

- Políticas claras y transparentes para la gestión de los conflictos (art.3).

- Acceso abierto a las publicaciones científicas y la publicación de los datos de investigación como garantía de transparencia en la gestión de la investigación, así como para garantizar la integridad científica y la transparencia en la gestión de la investigación (art.12).

- Transparencia en la gestión de los recursos públicos y rendición de cuentas mediante auditorías periódicas y publicación de los informes de auditoría (arts.53 y 59).

2.5.- Beneficios de la transparencia en el ámbito universitario

La transparencia es esencial en el ámbito universitario por varias razones:

En primer lugar, mejora la calidad de la educación al permitir a la comunidad universitaria y a la sociedad conocer su funcionamiento, objetivos y resultados.

En segundo lugar, genera confianza en las instituciones educativas al conocer cómo se utilizan los recursos y cómo se toman las decisiones.

En tercer lugar, rinden cuentas sobre su actividad, especialmente relevante en el ámbito de la gestión económica y financiera de las universidades, ya que es necesario que se publiquen de forma periódica y accesible las cuentas y presupuestos de la institución. La publicidad de esta información es una garantía de que los recursos se están utilizando de forma adecuada y transparente, y se pueden detectar posibles irregularidades o malas praxis.

Por último, la participación de los estudiantes en los procesos de toma de decisiones. Para ello, es necesario que existan mecanismos de consulta y participación como en el Claustro Universitario, Consejo de Gobierno, Consejo Social y Consejo de Estudiantes.

En conclusión, la transparencia de los poderes públicos es un indicador de la calidad democrática de un Estado (Girón Reguera, 2017, 458-461), contribuye a que los

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

ciudadanos no sólo estén mejor informados, sino que se sientan animados a colaborar y participar en la gestión de los recursos públicos, y, en el caso concreto de las Universidades, mejora la eficiencia de las Universidades, reduce los costes en los procesos, y, por otro lado, al abrir y compartir la información pública, permite que la misma se pueda reutilizar (Ramón Fernández, 2015, 344-346) con los beneficios económicos que ello representa para el sector privado (Villoria, 2014-2015, 96).

3.- Protección de datos personales en el ámbito universitario

3.1.- El tratamiento de los datos personales

La protección de datos personales es un derecho fundamental, garantizado en el art. 18.4 de nuestro texto constitucional, y que está reconocido en la legislación de la mayoría de los países democráticos (Arenas, 2006; y Arenas, 2022), siendo en el ámbito universitario donde la protección de datos adquiere una especial dimensión debido a la gran cantidad de información de carácter personal que manejan, como datos personales identificativos, académicos, profesionales o financieros.

Las instituciones universitarias, como responsables del tratamiento conforme con lo dispuesto en el 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 (RGPD)[16], deben garantizar la protección de los datos personales de los miembros de la comunidad universitaria y de cualquier ciudadano que haya facilitado información a la institución. Para ello, deben adoptar medidas de seguridad y cumplir con la normativa vigente en materia de protección de datos.

Las Universidades, a la hora de manejar datos personales y saber que los tendrá que hacer públicos para mejorar sus servicios y cumplir con la exigencia de transparencia, deberán diseñar los mismos con arreglo a los principios de "protección de datos por defecto" y "desde el diseño", esto es, tratando el estricto número de datos personales necesarios para el servicio que se va a prestar, ni uno más ni uno menos, y haciendo una valoración de cómo el servicio que se va a ofrecer va a afectar a la privacidad de los sujetos implicados, diseñándolo de tal manera que les afecte lo menos posible (Considerando 78 RGPD y arts. 5 y 25 RGPD). Que un dato se vuelva accesible por un interés público no significa que el sujeto afectado deba perder su privacidad o el control sobre los mismos.

[16] Vid. Art. 4.7) RGPD definición de «responsable del tratamiento» o «responsable».

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

3.2.- Protección de datos en la LOSU

A pesar de que tanto el RGPD como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)[17] tienen ya varios años de vigencia, no se había regulado ni adaptado el ámbito universitario, tales normas, máxime teniendo en cuenta que incluso la propia LOPDGDD habla de derechos digitales que debe ser regulados como así como la adaptación de los planes de estudios y de las competencias de los docentes[18].

Este derecho fundamental se recogió someramente en la Disposición adicional vigésima primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modificaba la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, en la que se regulaba, de conformidad con la, en su día vigente, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), cuestiones como la necesidad de recoger el consentimiento en algunas cuestiones referidas a los estudiantes y al personal de las universidades, el contenido de los currículos y el contenido académico y científico de los currículos de los profesores e investigadores que las universidades, y las agencias o instituciones públicas de evaluación académica y científica pueden hacer público[19].

Dicho esto, el legislador debería haber abordado este tema tan trascendental en la nueva normativa del sistema universitario pero no ha sucedido y si comprobamos el

[17] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

[18] Art. 83 LOPDGDD.

[19] Dado que no es una norma fácilmente accesible y que ya se encuentra derogada reproducimos aquí la Disposición Adicional Vigésima primera LO 4/2007: "Protección de datos de carácter personal: 1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica. Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados. 2. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido de los currículos a los que se refieren los artículos 57.2 y 62.3. 3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación. 4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación. 5. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos de los profesores e investigadores que las universidades y las agencias o instituciones públicas de evaluación académica y científica pueden hacer público, no siendo preciso en este caso el consentimiento previo de los profesores o investigadores".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

Dosier documental del Proyecto disponible sobre la LOSU podremos comprobar como tampoco se realizó siquiera un análisis sobre la normativa de protección de datos, ni se menciona la posibilidad de consulta a la Agencia Española de Protección de Datos (AEPD) o a CRUE Universidades Españolas[20].

Esto es un hecho lamentable porque el legislador ignora la debida regulación que se debe realizar de un derecho fundamental más aún ante el auge imparable de la tecnología y de la inteligencia artificial que está cambiando el paradigma de la enseñanza tanto en la forma como en el fondo del sistema educativo.

Tampoco hay constancia de que se solicitará un informe a la Agencia Española de Protección de Datos con el objeto de que hubiese asesorado e informado sobre el contenido de la norma en relación con las incompatibilidades, ausencias o sugerencias sobre su ámbito de competencia.

Por otro lado, el Grupo de Trabajo de Delegados de protección de datos creado dentro de la Sectorial de Secretarías Generales de CRUE Universidades Españolas, fue advirtiendo de esta falta de regulación específica. Debemos señalar aquí que dicho Grupo de Trabajo estaba compuesto por un grupo de Delegados/as de Universidades españolas de toda España y del sector público y del privado, por lo que sus conclusiones son una muestra representativa del sentir del colectivo de Delegados/as de Protección de Datos de Universidades de toda España.

Es por ello que este Grupo de Delegados/as de Protección de Datos realizó una "Propuesta de inclusión de un marco normativo específico de protección de datos en la LOSU" en la que se realizó una justificación de la propuesta así como un artículo de mínimos para su inclusión como disposición adicional. Este Informe manifestaba lo siguiente[21]:

"Las universidades se caracterizan por ser instituciones de naturaleza compleja, tanto en su estructura como en su modelo de gestión y en los fines que persiguen. Desde este punto de vista, junto con sus tareas naturales vinculadas a la investigación y la docencia, la institución universitaria presta servicios de la más variada naturaleza tanto a los miembros de la comunidad universitaria como a los terceros que, en el día a día organizativo, se relacionan con la misma. El despliegue ordinario de sus funciones se articula a través de múltiples procesos de gestión que implican tratamientos de datos personales de muy diversa índole.

[20] Vid. Información del Proyecto de Ley; Dosier documental y Audiencia e información pública.

[21] A pesar de su extensión, reproducimos aquí literalmente las conclusiones alcanzadas por el citado Grupo de DPDs, por no personalizar el trabajo desarrollado en el seno del mismo y por no tergiversar las palabras allí vertidas.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

El 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 (RGPD), junto con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) son las normas que definen, con carácter general, los principios, habilitaciones y condiciones conforme a los cuales los datos personales pueden y deben ser tratados por cualquier entidad, lo que incluye a las universidades públicas y privadas, sin perjuicio de la especificidad que la universidad privada tiene en esta materia.

Sin perjuicio del margen de apreciación nacional y del hecho de que los Estados no podrán legislar aquellas materias reservadas al citado RGPD, lo cierto es que dicha norma contiene numerosas remisiones legislativas que implican la necesidad de que las habilitaciones para tratar datos personales se deban encontrar en la propia legislación nacional. No obstante, desde el punto de vista de la técnica legislativa, las referencias a la materia de protección de datos suelen consistir en referencias de carácter genérico relativas al deber de cumplir con la legislación vigente en la materia. Ello obliga en no pocas ocasiones a las universidades y a sus delegados/as de protección de datos a desplegar una labor interpretativa altamente costosa, y en la mayor parte de los casos insegura, a la hora de definir criterios que legitimen el tratamiento de los datos de carácter personal, no siendo admisible, como bien ha señalado el Comité Europeo de Protección de Datos, recurrir al consentimiento como base de legitimación. Estas dificultades e inconsistencias se evidenciaron de modo particularmente significativo en el proceso de migración acelerada al trabajo a distancia, y a la docencia y a la realización de exámenes online durante el periodo confinamiento provocado con la declaración del estado de alarma por la pandemia por COVID-19. Todo ello es lo que llevó al Grupo de Trabajo de Delegados/as de Protección de Datos de la CRUE, con un enorme esfuerzo interpretativo, a elaborar, durante los primeros meses de la pandemia, todo un conjunto de documentos para hacer frente a la inseguridad jurídica existente.

La universidad del futuro se enfrenta a significativas oportunidades y, también, a riesgos de la mano de la transformación digital. Sería recomendable que, en el marco de una potencial reforma de la actual Ley Orgánica 6/2001 de Universidades (LOU), el Ministerio competente contribuyera a crear seguridad jurídica a la hora de tratar datos en y por la Universidad y tuviera en consideración el impacto en ámbitos como la gestión de recursos humanos y la investigación científica, debiendo llevar a cabo una relectura de la futura norma -como exige el RGPD y nuestra LOPDGDD- desde el punto de vista de la protección de datos desde el diseño y por defecto, contando con la integración de expertos en la materia en sus grupos de trabajo.

Así las cosas, ante las carencias de la actual legislación universitaria en este terreno y la anunciada reforma de la LOU, el Grupo de Trabajo de Delegados/as de

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

Protección de Datos de la CRUE ha considerado que resultaría particularmente conveniente que el legislador tuviera en cuenta las necesidades derivadas de los tratamientos de datos en el contexto del despliegue de los fines y funciones de la universidad con el objetivo de dotar de seguridad jurídica al sistema, identificando aquellos tratamientos que, por su carácter estratégico, o por su alto grado de sensibilidad, necesitan de un desarrollo o mención específica".

3.3.- Propuesta normativa

Como resultado del Informe citado anteriormente se elaboró una propuesta de Disposición adicional de Protección de datos de carácter personal que recogía una disposición de mínimos[22]:

"1. Se aplicará a los tratamientos de datos personales derivados de lo dispuesto en la presente Ley Orgánica, la normativa vigente en materia de protección de datos, así como sus normas de desarrollo.

2. No requerirán el consentimiento de las personas interesadas los tratamientos de datos personales que realicen las universidades en el ejercicio de las funciones que tienen atribuidas por ley, entre otros, en los siguientes casos:

a) Para los tratamientos de datos personales vinculados a los procesos de gestión administrativa, de gestión de la docencia, evaluación de los aprendizajes y comprobación de los conocimientos adquiridos. La publicación de los resultados deberá realizarse con las garantías correspondientes y en entornos institucionales y cerrados de comunicación, preferentemente de carácter electrónico y de acceso restringido a los sujetos participantes.

b) Para la evaluación de la calidad administrativa, docente o investigadora en los casos previstos legalmente, así como para la publicación de sus resultados y del contenido académico y científico de los currícula en los casos en que así se establezca.

3. Se regirán por lo previsto en la normativa vigente en materia de protección de datos las actividades de carácter investigador, incluidas las académicas llevadas a cabo por las/los estudiantes. Estas actividades de carácter investigador serán lícitas cuando traten cualquier categoría especial de datos y se rijan, además, por los criterios y garantías previstos en la Disposición Adicional Decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Las universidades dispondrán de protocolos o patrones de privacidad que aseguren el cumplimiento normativo en esta materia incluyendo, entre otros, la formación obligatoria del personal, la disposición de una sección

22 Con la misma justificación que en el caso anterior, reproducimos aquí, a pesar de su extensión la propuesta presentada por el Grupo de DPDs de la CRUE.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

específica para estos tratamientos en el registro de actividades del tratamiento, la aplicación de metodologías de protección de datos desde el diseño y por defecto, la garantía del origen legítimo de los datos y la aplicación del principio de proporcionalidad. En todo caso, se deberá contar con el soporte del delegado/a de protección de datos.

En ningún caso se podrá obligar a los miembros de la comunidad universitaria a participar en calidad de sujetos en una investigación.

4. La universidad tendrá la consideración de responsable del tratamiento o encargado del tratamiento en las actividades de investigación con datos realizadas por los miembros de la comunidad universitaria. El miembro de la comunidad universitaria que despliegue actividades de tratamiento con fines de investigación por propia iniciativa, no comunicando o incumpliendo los protocolos definidos por la universidad será considerado responsable del tratamiento.

5. Las transferencias internacionales de datos, que sean necesarias en el ejercicio de las funciones que la universidad tiene atribuidas por ley, con un tercer país u organización internacional, en ausencia de una decisión de adecuación, podrán llevarse a cabo siempre y cuando exista el preceptivo convenio de colaboración u otro tipo de instrumento que aporte las garantías adecuadas.

6. Las universidades llevarán a cabo, en el plazo máximo de dos años desde la entrada en vigor de esta norma, actividades específicas de formación obligatoria de su personal y contemplarán en sus planes de estudio enseñanzas conducentes a la obtención de competencias sobre el correcto tratamiento de los datos personales, el uso y seguridad de los medios digitales y las garantías de los derechos fundamentales en Internet. A estos efectos se contará con el asesoramiento del delegado/a de protección de datos".

El arduo esfuerzo de trabajo realizado para llegar a un consenso fue inocuo por cuanto no hay constancia de que esta propuesta de disposición, junto a su informe, fuera siquiera debatida en el seno de la CRUE, ni aparece publicado en su web, como sí que figuran otros textos realizados por este Grupo de trabajo.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

4.-¿Avance o retroceso en materia de transparencia y protección de datos en la LOSU?

4.1.- Reflexión en cuanto a los sujetos obligados, desde una doble óptica, LOSU y LTAIBG

En la mayor parte del articulado de la LOSU, la norma se refiere, y regula, los derechos y obligaciones, especialmente en materia de transparencia de las Universidades Públicas, pero creemos que debería existir una mayor obligación hacia las Universidades privadas, y que se debería modificar en este sentido la LTAIBG.

Las Universidades privadas, al igual que las públicas y los centros privados adscritos a éstas, prestan el mismo servicio público de educación superior. De hecho, el artículo 1.2 LOSU declara que se entiende por sistema universitario el conjunto de universidades, públicas y privadas, y de los centros y estructuras que les sirven para el desarrollo de sus funciones.

Más aún, por si existiera alguna duda, el artículo 95.1 LOSU declara que "Las universidades privadas tendrán personalidad jurídica propia en cualquiera de las formas legalmente existentes, pudiendo ser entidades con ánimo de lucro o de carácter social, incluidas las sociedades cooperativas. Su objeto social exclusivo será la educación superior y la investigación y, en su caso, la transferencia e intercambio del conocimiento. Deberán realizar todas las funciones a las que se refiere el artículo 2.2".

En este sentido, el profesor Fernández indica que "es evidente que si las Universidades privadas son receptoras de ayudas públicas, en las condiciones establecidas en el art. 3.b) LTAIBG, deberán cumplir la Ley como cualquier otra entidad privada. Pero la principal cuestión es determinar si es o no de aplicación en este ámbito la antes indicada obligación de suministrar información del artículo 4 LTAIBG. Las Universidades privadas…prestan el mismo servicio público de la educación superior. De hecho, cuando el artículo 1.1 de la LOU declara que la Universidad realiza el servicio público de la educación superior, no diferencia entre universidades públicas y privadas. Más aún, por si existiera alguna duda, el artículo 2.1 declara que el objeto social exclusivo de las Universidades privadas será la educación superior mediante la realización de las funciones que el artículo 1.2 asigna a la Universidad al servicio de la sociedad (exigencia que reitera el artículo 3.2). Por tanto, parece evidente que las Universidades privadas son entidades privadas que prestan un servicio público, de modo que se cumple la premisa básica del artículo 4 LTAIBG…pero aun cuando las Universidades privadas tienen por objeto exclusivo la prestación de un servicio público y, por ello, puede decirse que su actividad es

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

materialmente pública, el artículo 4 LTAIBG no es operativo, debido a la indicada exigencia de vinculación a una entidad pública" (Fernández, 2022, 34-35).

Asimismo, corresponde a la Administración de la Comunidad Autónoma regular los mecanismos de inspección necesarios (art. 100.5 LOSU[23]) pero se trata de un control de legalidad. Así, aun cuando las Universidades privadas tienen por objeto la prestación de un servicio público, el artículo 4 LTAIBG no es operativo debido a la indicada exigencia de vinculación a una entidad pública. Pero es más, en el último párrafo del art. 100.5 LOSU, se indica expresamente que "las Comunidades Autónomas podrán regular las obligaciones de transparencia en la gestión de las universidades privadas", dejando claramente sin efecto la regulación del citado artículo 4 LTAIBG para estas universidades.

Por tanto, compartimos la opinión del profesor Fernández en el sentido de que el artículo 4 LTAIBG debería actualizarse para que las Universidades privadas, como gestoras del servicio público de la educación superior, pudieran quedar sometidas al cumplimiento de esta Ley.

4.2.- ¿Incompatibilidad entre transparencia y protección de datos?

El principio de transparencia y la protección de datos a menudo pueden parecer encontrarse en conflicto, ya que ambos tienen objetivos y requisitos diferentes, pero, en contra de lo que se piensa, podemos afirmar que ambos son complementarios. En este sentido, como indica el profesor Piñar, "un desequilibrio entre ambas, en favor de una u otra, puede llevar a situaciones realmente no deseables" (Piñar, 2014, 13).

El principio de transparencia en las Universidades es una realidad inevitable, así como el empleo de las herramientas que nos ofrecen los avances tecnológicos que permiten y favorecen el tratamiento de la información. En un ámbito como es el universitario, la apertura del conocimiento al resto de la sociedad constituye parte de su esencia, pero esto debe encontrar su justo equilibrio con el respeto a la privacidad de los sujetos, por lo que debemos encontrar "la cultura del equilibrio entre dos valores absolutamente imprescindibles para el desarrollo democrático de cualquier país" (Piñar, 2014, 13).

Es por ello indispensable encontrar ese equilibrio entre el principio de transparencia y un adecuado tratamiento de datos personales, ello generará un nivel de confianza

[23] El artículo 100.5 LOSU dispone que "En el marco de la normativa estatal, las Comunidades Autónomas regularán los mecanismos de inspección necesarios de las universidades privadas y podrán requerir, a tal efecto, cualquier tipo de información económico-financiera de las mismas y de los centros privados adscritos a universidades públicas. De igual modo, podrán regular las obligaciones de transparencia en la gestión de las universidades privadas".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

necesario para poder transmitir la información, para hacerla pública y cumplir así con la exigencia de transparencia necesaria en una Administración pública moderna.

En algunos casos, la transparencia puede requerir que las organizaciones divulguen una cantidad significativa de información sobre el procesamiento de datos, lo que puede entrar en conflicto con la protección de datos. Por ejemplo, si una organización tiene que ser completamente transparente y revelar todos los detalles sobre el procesamiento de datos, incluidos los datos personales sensibles, esto podría poner en riesgo la privacidad y la seguridad de los individuos.

Sin embargo es posible encontrar un equilibrio adecuado para garantizar la privacidad y los derechos de los individuos sin comprometer la divulgación de información clara y comprensible sobre el procesamiento de datos. De hecho, la propia LTAIBG dispone en su articulado de un precepto destinado a buscar el equilibrio y a establecer unos criterios de ponderación cuando entre las obligaciones de transparencia y derecho de acceso a la información pública nos encontramos con datos personales[24] (Troncoso, 2017; y Arenas, 2020).

4.3.- Desafíos de la transparencia en el ámbito universitario

Después de veintidós años desde que entrara en vigor la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (LOU), y de diez años desde que lo hiciera la LTAIBG, es indudable -sería preocupante lo contrario- que se han realizado avances en materia de transparencia.

Ciertamente, la LOU se aprobó antes de la entrada en vigor de la LTAIBG en el 2013, pero ni la modificación operada en el año 2007 -y que introdujo la referencia a la normativa de protección de datos- aventuró la importancia de que las Universidades, como Administraciones públicas, tuvieran que verse sometidas al principio de publicidad que constitucionalmente se les impone a éstas. Y tras el 2013, hasta la actualidad, esa obligación sigue sin recogerse en la normativa universitaria. La LOSU incluye, como ha quedado dicho, referencias a la exigencia de transparencia en ámbitos a los que la LOU no prestaba especial atención, como es lo relacionado con la transferencia de conocimiento, pero la necesidad de transparencia en aspectos cruciales como los que se mencionan a continuación y que la LOU obviaba, siguen sin plasmarse en el papel. Una oportunidad perdida, como lo ha sido en el terreno de adaptar nuestras Universidades a los avances tecnológicos.

A pesar de haberse avanzado en la inclusión o mención de la transparencia en la regulación de la nueva normativa universitaria, su implementación sigue presentando desafíos porque algunas cuestiones no se han abordado con la

[24] Art. 15 LTAIBG.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

suficiente claridad, o no se han propuesto medidas concretas, dejando a las Comunidades Autónomas o a las propias universidades su regulación, y sin plantear una propuesta financiera real para abordar estos desafíos.

En nuestra opinión la LOSU es una normativa de mínimos, como así se indica en su Preámbulo cuando manifiesta que "Esta ley orgánica no quiere imponer soluciones ni trazar caminos concretos en que todo ello deba resolverse. Busca abrir posibilidades, facilitar conexiones… En esta línea, la ley establece un mínimo común denominador, habilitando un amplio margen al desarrollo de sus disposiciones mediante la labor normativa de las Comunidades Autónomas y las concreciones de los Estatutos y normas de organización y funcionamiento de las propias universidades".

La implementación de lo dispuesto en la LOSU puede requerir recursos adicionales, como personal, tecnología y financiación, y no se ha indicado ni cómo ni de dónde van a salir esos recursos que conllevan un coste económico, trasladando su solución a las Comunidades Autónomas.

Otro de los desafíos a resolver es la endogamia que existe en la universidad, por ejemplo, en lo referente a los concursos de los cuerpos docentes universitarios. Esto no se va a solucionar con comisiones de selección integradas por una mayoría de miembros externos a la universidad convocante, elegidos por sorteo público entre el conjunto del profesorado y personal investigador de igual o superior categoría a la plaza convocada (art. 71.1.b) LOSU). El papel lo soporta todo, pero esta propuesta es una quimera, una declaración de intenciones que no va a solucionar el problema real, en una comunidad universitaria donde todos se conocen y que, como toda Administración pública, debería regirse por los principios de mérito y capacidad previstos constitucionalmente.

Las universidades tendrán que elaborar nuevos Estatutos en los que cada una regule las funciones, estructuras, composición y porcentajes de representación de los órganos colegiados (Claustro universitario, Consejo de Gobierno, Consejo Social, Consejo de Estudiantes y otros órganos colegiados), pero, además, cada Comunidad Autónoma tendrá la potestad de presentar diferentes y variadas tipologías de profesorado, de becas, de acreditaciones, de tasas, de estatutos, de claustros, lo que podría llevar a desigualdades, falta de equidad y homogeneidad.

Igualmente, no nos parece transparente que la designación del Rector o de la Rectora se lleve a cabo por el procedimiento, y con los requisitos de méritos y experiencia, que determinen los Estatutos de cada Universidad. Entendemos que esto debería haber quedado regulado expresamente en la LOSU para que no hubiese intereses políticos ni partidistas. Esto hubiese dado mayores garantías de transparencia a esta designación del puesto más importante y representativo de la universidad.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

Por último, creemos que es difícil una transparencia real y objetiva si se permite que los Claustros puedan analizar y debatir otras temáticas de especial trascendencia (art. 45.2.g) LOSU) con una clara simbología política y que parece romper con lo que la Universidad debe ser: una institución que desarrolle funciones centrales de docencia, investigación y transferencia e intercambio del conocimiento.

4.4.- Desafíos en el desarrollo de la protección de datos en el ámbito universitario

Al contrario de los avances en materia de transparencia, aunque tibios, estos no se han dado en el desarrollo de la protección de datos.

Ya la LOPDGDD, en su artículo 83, relativo al Derecho a la educación digital, planteaba lo siguiente en sus apartados 1 y 3:

"1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

(...)

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet."

Nada de esto se ha mencionado siquiera en la LOSU ni ha tenido un desarrollo reglamentario desde la aprobación de la LOPGDD en el año 2018.

Igualmente tampoco se ha afrontado el gran reto que supone el tratamiento de datos en los proyectos de investigación y/o en los TFG, TFM o Tesis doctorales, aclarar bases de legitimación en el tratamiento de datos personales o especificar algunos servicios que en el futuro van a requerir el tratamiento de datos biométricos, con la consecuente necesidad de realizar el oportuno análisis y evaluación de impacto. Ni se hace alusión a su posible conflicto con las obligaciones de transparencia o a los criterios de resolución previstos en la LTAIBG.

En conclusión, es urgente acometer un desarrollo legal o reglamentario de estas cuestiones para poder afrontar una utilización de datos personales con las debidas garantías, que garantice la aplicación de este derecho fundamental como sinónimo de una sociedad democrática fuerte, y que quiere afrontar los importantes retos que

CC BY SA

DOI: https://doi.org/10.51915/ret.311

nos esperan no solo en el mundo universitario sino en todos los ámbitos, con la irrupción implacable y veloz de la inteligencia artificial que cambiará nuestro paradigma como sociedad. Nos dará largo y tendido para seguir debatiendo, construyendo e investigando.

Bibliografía

ARENAS RAMIRO, M. (2006) El derecho fundamental a la protección de datos en Europa. Valencia: Tirant lo Blanch.

ARENAS RAMIRO, M. (2016), "Transparencia, acceso a la información pública y democracia: elementos inseparables", en Revista Transparencia & Sociedad, nº 4, pp. 113-131.

ARENAS RAMIRO, M. (2020), "Transparencia y protección de datos personales en el ámbito universitario: hacia una Universidad abierta", en Revista CEF Legal, nº 230, pp. 107-134.

ARENAS RAMIRO, M. (2022) "Data protection in Latin America", en GLORIA GONZÁLEZ FUSTER/ROSAMUNDE VAN BRAKEL / PAUL DE HERT (Eds.), Research Handbook on privacy and data protection law. Reino Unido: Edwar Elgar Publishing, pp. 139-160.

BARSTOW, R. y JOHNSON, A. (2016) "Transparencia en la Universidad", Derecom, nº 20.

BURGAR ARQUIMBAU, J.M. (2015) "Acceso a la información pública y protección de datos de carácter personal en el marco de la Ley de Transparencia: graduación y ponderación". En COTINO HUESO, L., SAHUQUILLO OROZCO, J.L., CORREDOIRA Y ALFONSO, L. 2015. El paradigma del gobierno abierto: retos y oportunidades de la participación, transparencia y colaboración, pp. 206-219.

CASARES MARCO, A.B. (2018) "Gobernanza universitaria", en Boujaddaine, M. (Ed.), La gouvernance et l`enjeu de concilier l´éthique et la performance, EUNSA, Navarra.

COUSIDO-GONZALEZ, P. (2022) "La transparencia en las Universidades españolas. A 7 años de la ley 19/2013" en Revista Ius et Praxis, nº. 2, pp. 25-43.

FERNÁNDEZ RAMOS, S. (2022) "Universidad y transparencia: los sujetos obligados", en Revista Española de la Transparencia, nº. 14, pp. 25-36.

GARCÍA GARCÍA, J. (2014). "Gobierno abierto: transparencia, participación y colaboración en las Administraciones Públicas", en Innovar, 24 (54).

GARCÍA MUÑOZ, J., ARIAS RODRÍGUEZ, A., CHAVES GARCÍA, J.R., ISABEL CARO, A. (2023) "Gestión y fiscalización de la investigación en el ámbito universitario", en

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

RIVERO ORTEGA, R. 2023. La reforma universitaria de 2023. Comentarios a la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario, pp.99-232.

GIRÓN REGUERA, E (2017). "Comentario artículo 5 LT: la transparencia activa de las Administraciones y entidades públicas", en TRONCOSO REIGADA, A. 2017. Comentario a la Ley de Transparencia, Acceso a la información pública y Buen Gobierno. Civitas. pp. 457-469.

GUICHOT, E. (2018) "Transparencia y protección de datos en las universidades públicas", en Revista española de derecho administrativo, nº 193, pp. 85-126.

LIZCANO ÁLVAREZ, J. (2013-2014). "Transparencia", en Eunomía, nº 3.

MARTIN CAVANNA, J. (2017) "Cómo incentivar la transparencia voluntaria por medio de instituciones independientes", en TRONCOSO REIGADA, A. 2017. Comentario a la Ley de Transparencia, Acceso a la información pública y Buen Gobierno. Civitas. pp. 408-439.

PALOMARES HERRERA, M. (2022). Fundamentos de la Transparencia y el acceso a la información.

PARRA SÁEZ. S. (2015) "Transparencia y protección de datos destinados a entenderse", en COTINO HUESO, L., SAHUQUILLO OROZCO, J.L., CORREDOIRA Y ALFONSO, L. El paradigma del gobierno abierto: retos y oportunidades de la participación, transparencia y colaboración.

PÉREZ CONCHILLO, E. (2023). Transparencia y derecho de acceso a la información pública: configuración y naturaleza constitucional.

PIÑAR MAÑAS, J.L. (2014). "Transparencia y derecho de acceso a la información pública", en Revista Catalana de Dret Public, nº 49.

RAMÓN FERNÁNDEZ, P., (2015). "Tratamiento legislativo del principio de reutilización en la legislación de transparencia: algunas cuestiones" en COTINO HUESO, L., SAHUQUILLO OROZCO, J.L., CORREDOIRA Y ALFONSO, L., El paradigma del gobierno abierto: retos y oportunidades de la participación, transparencia y colaboración.

RODRÍGUEZ-ARANA, J. (2013). "La buena Administración como principio y como derecho fundamental en Europa", en Revista Misión Jurídica. Vol. 6, núm. 6, pp. 23-56.

TOMÁS MALLÉN, B. (2004) El derecho fundamental a una buena Administración. Madrid: INAP.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia y protección de datos personales en el ámbito universitario ¿avance o retroceso?
por David Díaz Lima
Págs. 201-224
DOI: https://doi.org/10.51915/ret.311

TRONCOSO REIGADA, A. (2006) "La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos personales en las Universidades", en Revista de Derecho Político, nº 67.

TRONCOSO REIGADA, A. (2017) "La protección de datos personales como límite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 – Protección de datos personales", en TRONCOSO REIGADA, A., Comentario a la Ley de Transparencia, Acceso a la información pública y Buen Gobierno. Civitas, pp. 959-1078.

TRONCOSO REIGADA, A. (2017). Comentario a la Ley de Transparencia, Acceso a la información pública y Buen Gobierno. Civitas.

ZAPICO, E. (2013). "El control por resultados en la gestión pública desde la perspectiva ciudadana", en Palomar, A. y Garcés, M. (Dirs.), La gestión de los fondos públicos: Control y responsabilidades, Aranzadi, Navarra.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Las obligaciones de transparencia de las Autoridades de protección de datos: un requisito indispensable para su independencia

Mónica Arenas Ramiro[1]
Universidad de Alcalá
España

ORCID: 0000-0002-9329-2246

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

Este trabajo ha sido realizado en el marco del proyecto del Ministerio de Ciencia e Innovación DATATRANSCO con referencia n.º PID2021-128309NB-I00.

RESUMEN: El derecho fundamental a la protección de datos personales goza de una garantía adicional a los tradicionales mecanismos de garantía de los derechos fundamentales como son las Autoridades de control. Nos centraremos aquí en analizar el porqué de su existencia, su organización y funciones. El objetivo es constatar la necesidad de que estas Autoridades administrativas independientes cumplan con las exigencias de transparencia no sólo por ser Administraciones públicas, sino porque por su especial naturaleza jurídica y su carácter independiente se han convertido en una realidad necesaria en las sociedades actuales, reforzando, en último término, la garantía de derechos fundamentales en el sector que regulan o asesoran, fortaleciendo así nuestros Estados.

PALABRAS CLAVE: Autoridades de control, Autoridades administrativas independientes, Datos personales, Transparencia, Protección de datos.

[1] Profesora contratada doctora de Derecho Constitucional de la Universidad de Alcalá. Sobre sus principales líneas de investigación ha publicado obras relacionadas con protección de datos personales, redes sociales, medios de comunicación, transparencia, partidos políticos, sociedad digital, igualdad y género, derechos digitales e inteligencia artificial.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

CONTENIDOS: 1.-Introducción. 2.-Las autoridades de control. *2.1.-Autoridades administrativas independientes como garantes del derecho fundamental a la protección de datos personales.* 2.1.1.-Objetivo: la protección de los derechos fundamentales. 2.1.2.-Las autoridades de control en España. *2.2.-Organización, composición y funcionamiento. 2.3.-Competencias y funciones.* 3.- Obligaciones de transparencia de las Autoridades de control. *3.1.- En las leyes de transparencia. 3.2.-En la normativa de protección de datos. 3.3.-Respecto de su organización, composición y funcionamiento. 3.4.-Respecto de sus competencias y funciones.* 4.-A modo de reflexión. – Bibliografía.

Transparency obligations of Data Protection Authorities: an indispensable requirement for their independence

ABSTRACT: The fundamental right to the protection of personal data enjoys an additional guarantee to the traditional mechanisms for guaranteeing fundamental rights, such as the supervisory authorities. We will focus here on analysing the reason for their existence, their organisation and functions. The objective is to confirm the need for these independent administrative authorities to comply with the requirements of transparency not only because they are public administrations, but also because their special legal nature and independent character have made them a necessary reality in today's societies, ultimately reinforcing the guarantee of fundamental rights in the sector they regulate or advise, thus strengthening our States.

KEYWORDS: Supervisory authorities, Independent public authorities, Personal data, Transparency, Data protection.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

1.- Introducción

El fenómeno de las Autoridades administrativas independientes en Europa tiene su origen -con sus matices- en Estados Unidos como Agencias reguladoras independientes. En 1887 se creó la *Interstate Commerce Commission* (ICC) con competencias en materia de comercio interestatal y de transportes con la finalidad inicial de combatir las malas prácticas y los abusos en el sector ferroviario, de fijar tarifas y de consagrar precios justos para defender así a los consumidores y garantizar sus derechos.[2] A partir de aquí, su creación en Europa no se dejó esperar, centrándose en proteger, en último término, derechos fundamentales de los ciudadanos en sectores conflictivos (por todos, Salvador Martínez, 2002; y, también, Pauner Chulvi y Tomás Mallén, 2009; Troncoso Reigada, 2009: 27-216; Blanco Antón, 2018: 591-607; y Betancor Rodríguez, 1994). Estas Autoridades surgieron para ordenar sectores de intervención pública especialmente sensibles (Pomed Sánchez, 1993: 169) y como una forma de "huída" del Derecho público, e incluso podríamos decir, como una forma de huir del Derecho constitucional (Rallo Lombarte, 2009: 11).

En el caso concreto del tratamiento de datos personales, la exigencia de crear "Autoridades" encargadas de controlar los tratamientos de datos personales se manifestó por primera vez en el ámbito del Consejo de Europa, por un lado, en el Convenio 108 sobre Protección de Datos de 1981 (aunque dicha obligación se concretó posteriormente en el 2001 en su Protocolo Adicional),[3] y, por otro lado, a través de la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH). Posteriormente, en la Unión Europea, la normativa comunitaria, en especial, la Directiva 95/46/CE sobre Protección de Datos Personales —hoy derogada—,[4] y la

[2] La Comisión de Comercio Interestatal (Interstate Commerce Commission) se aprobó por la Ley de Comercio Interestatal aprobada el 4 de febrero de 1887 (49 U.S.C. 10301 et seq.), y fue eliminada en 1995, pasando a ocuparse de sus funciones la Comisión de Transportes Terrestres (Surface Transportation Board).

[3] Vid. Art. 13 Convenio 108, relativo a la Cooperación entre las Partes. Esta obligación se concretó posteriormente en el 2001 en su Protocolo Adicional. El marco paneuropeo de protección de datos ha perfilado las garantías en el tratamiento de los datos personales dentro y fuera de Europa, convirtiéndose en un punto de referencia a nivel mundial. La actualización, en 2018, del Convenio 108 del Consejo de Europa de 28 de enero de 1981 (ahora comúnmente conocido como Convenio 108+) ha sido pieza clave y necesaria para los desarrollos normativos a nivel internacional y europeo en esta materia y para dar efectividad al derecho fundamental a la protección de datos. En 2021 se celebró la ratificación española del Protocolo Adicional que moderniza el Convenio, en el Día Internacional de la Protección de Datos, conmemorando, a su vez, el 40º aniversario de la adopción del mismo (Monica Martínez, 2021).

[4] Art. 28 Directiva 95/46/CE sobre Protección de Datos Personales.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Carta de Derechos Fundamentales de la Unión Europa (CDFUE),[5] exigieron, y exigen, a los Estados miembros la creación de este tipo de Autoridades independientes para garantizar el derecho fundamental a la protección de datos personales. De la misma forma que también lo ha exigido el Tribunal de Justicia de la Unión Europea (TJUE), como luego veremos. Actualmente es el Reglamento General de Protección de Datos (RGPD), la norma que a nivel europeo regula su creación, composición y funciones, como luego veremos.[6] La independencia se convertía así en "la clave de bóveda para garantizar una protección efectiva" del derecho fundamental a la protección de datos personales (García Mahamut, 2023: 185).

Fruto de esta obligación a nivel europeo, los Estados miembros han creado en sus respectivos ordenamientos jurídicos nacionales "Autoridades independientes" encargadas de controlar los tratamientos de datos personales y garantizar de esta forma el derecho a la protección de datos.[7]

Por último, dejamos aquí indicado que este tipo de garantía adicional e independiente se reproduce en Europa no sólo en cada uno de los Estados miembros de la Unión Europea, sino a nivel comunitario. Así, nos vamos a encontrar con dos figuras encargadas de garantizar el cumplimiento de la normativa de protección de datos por parte de las instituciones y órganos comunitarios y del propio Derecho a nivel europeo. Nos referimos al Supervisor Europeo de Protección

[5] Dispone el art. 8 CDFUE: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[6] Vid. 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).

[7] En la página web del CEPD, podemos encontrar las Autoridades de control de todos los Estados miembros, con sus direcciones web. Vid. https://edpb.europa.eu/about-edpb/about-edpb/members_es.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

de Datos (SEPD)[8] y al Comité Europeo de Protección de Datos (CEPD) (González Fuster, 2019: 161-180; y Cervera Navas, 2016: 527-538).[9]

La idea pues de Autoridades de control encargadas de garantizar el respeto de derechos fundamentales supone una herramienta especializada y preventiva en un determinado sector y adicional a los tradicionales mecanismos de garantía de los que gozan los derechos fundamentales.[10] No obstante, el hecho de que estas Autoridades sean consideradas Administraciones independientes y gocen de unas competencias y poderes específicos, se las dote de independencia, y escapen así del régimen tradicional del Derecho administrativo —derogando el principio de jerarquía (Pomed Sánchez, 1993: 169)— para poder cumplir con su finalidad, nos lleva a cuestionarnos el porqué de su existencia como rara avis que no encaja a la perfección con el tradicional sistema de separación de poderes (Pomed Sánchez, 1998: 168).

Por otro lado, más allá de la discusión sobre su encaje constitucional y su conveniencia en determinados ámbitos, debemos analizar, para el caso que aquí nos interesa, si el hecho de que sean autoridades administrativas las convierte en sujetos obligados por la normativa de transparencia vigente, lo que nos lleva a plantearnos la importancia de hacerlas cumplir con sus obligaciones de transparencia, con el fin de contribuir a mejorar no sólo su organización y funcionamiento, sino, en último término, a fortalecer el derecho fundamental que están destinadas a proteger y/o regular.

---

[8] En el 2001, y como desarrollo del mandato contenido en el art. 286 TCE, y también en la hoy derogada Directiva 95/46/CE sobre Protección de Datos Personales, se aprobó el hoy también derogado Reglamento 45/2001 sobre Protección de Datos Personales por parte de las instituciones y órganos comunitarios. En este Reglamento se crea, en su art. 32, una Administración independiente encargada de la protección de los datos personales, el "Supervisor Europeo de Protección de Datos", con lo cual se dota a la protección de datos personales de una garantía específica y reforzada. En la actualidad, la referencia al Reglamento 45/2001 debe entenderse hecha al Reglamento (UE) 2018/1725, del Parlamento europeo y del Consejo, de 23 de octubre, relativo a la protección de las personas físicas en lo que respecta al tratamiento personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se deroga el Reglamento (CE) nº 45/2001, que recoge la figura del SEPD en sus arts. 52 a 60.

[9] El citado CEPD, reconocido expresamente en los arts. 68 a 76 RGPD, tiene su antecedente directo en el conocido como "G29" o Grupo de trabajo establecido en el art. 29 de la derogada Directiva 95/46/CE, aunque a diferencia del G29 el CEPD tiene personalidad jurídica propia.

[10] Con carácter general, y al margen de las diferencias típicas de los correspondientes ordenamientos jurídicos, ante una violación del derecho a la protección de datos personales su titular puede acudir a las siguientes vías: la vía judicial ordinaria, los Tribunales Constitucionales, el Defensor del Pueblo, el recurso ante el Tribunal Europeo de Derechos Humanos (TEDH), y el recurso ante el Tribunal de Justicia de la Unión Europea (TJUE).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

En este caso, nos centraremos en analizar las Autoridades de control creadas en relación con el derecho fundamental a la protección de datos personales y, específicamente, las Autoridades de control de protección de datos personales y, más concretamente, de las creadas en España. De hecho, nuestro Tribunal Constitucional señaló que este derecho, frente a la nueva realidad derivada del progreso tecnológico, requería para ello de una protección reforzada a través del establecimiento de Autoridades de control independientes (Salvador Martínez, 2002: 270-271).[11]

Estas Autoridades deben cumplir, esencialmente, con los principios de independencia en su organización y funcionamiento, pero como mecanismos de garantía de esta independencia, y como entes administrativos que son, también deberán cumplir con la exigencia de transparencia, con el fin de garantizar así el principio y derecho fundamental a una buena Administración. No podemos olvidar que una buena Administración es una Administración transparente, respondiendo a los principios de eficacia y eficiencia reconocidos constitucionalmente en el art. 103.1 CE. Así, veremos cómo la legislación sobre transparencia somete a estas Administraciones independientes a su ámbito subjetivo de aplicación. Se hace necesario analizar, por la especial trascendencia de estas Autoridades administrativas, si cumplen o no con sus obligaciones de transparencia, y cómo la ausencia de la misma afecta en último término al derecho fundamental, en este caso, a la protección de datos personales.

2.- Las Autoridades de control

En el sector del tratamiento de datos personales ya hemos explicado cómo surgieron estas Autoridades y cómo no sólo a nivel legislativo, sino también jurisprudencialmente, se ha venido reconociendo su necesidad como garantía del derecho fundamental a la protección de datos personales.

El derecho fundamental a la protección de datos personales se reconoce expresamente como tal en el ya citado art. 8 CDFUE y, a nivel nacional, en el art. 18.4 CE -diferenciado del derecho a la intimidad, como dijo expresamente la STC 290/2000- como un poder de disposición de los propios datos personales. Asimismo, fruto del mandato legislativo del citado art. 18.4 CE, en España se fueron aprobando distintas normas para regular el tratamiento de datos personales que van a reconocer la necesidad de creación de las Autoridades de control para garantizar el citado derecho.

Este tipo de Autoridades son muy variadas: en función de su composición, ya que algunas son órganos colegiados y otros órganos unipersonales; en función de su

[11] STC 292/2000, FJ 4º.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

grado de independencia funcional, dependiendo de si ejercen sus funciones dentro de la estructura de algún otro órgano administrativo o no; y en función de las competencias de la Autoridad. No obstante, con carácter general se puede decir que en Europa se ha optado, claramente, por la creación de un órgano especializado e independiente para la garantía del derecho a la protección de los datos personales.

Asimismo, en España, de la misma forma que a nivel central se creó una Autoridad independiente encargada de garantizar el derecho a la protección de datos personales, la AEPD, a nivel autonómico algunas Comunidades Autónomas también crearon sus Autoridades independientes, esto es, sus Agencias de Protección de Datos autonómicas. Nos referimos a las actuales Autoridades de control de Cataluña, País Vasco y Andalucía —y a la desaparecida Autoridad madrileña—.

2.1.- Autoridades administrativas independientes como garantes del derecho fundamental a la protección de datos personales

Ya ha quedado dicho que el derecho fundamental a la protección de datos personales, por un lado, se reconoce a nivel europeo en el art. 8 CDFUE y a nivel nacional en el art. 18.4 CE, estando actualmente desarrollado por la LO 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), y la LO 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.[12] Y, por otro lado, que este derecho está garantizado por una Autoridad de control independiente, teniendo ésta la naturaleza de una Autoridad administrativa independiente.

La Ley 40/2015, del Régimen Jurídico del Sector público (LRJSP) dedica a las Autoridades administrativas independientes el Cap. IV de su Tít. II relativo a la organización y funcionamiento del sector público institucional (arts. 109 y 110), y las define como "entidades de derecho público que, vinculadas a la Administración General del Estado y con personalidad jurídica propia, tienen atribuidas funciones de regulación o supervisión de carácter externo sobre sectores económicos o actividades determinadas, por requerir su desempeño de independencia funcional

[12] La LOPDGG surge para completar lo dispuesto en el citado RGPD y la LO 7/2021 es transposición de Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

o una especial autonomía respecto de la Administración General del Estado, lo que deberá determinarse en una norma con rango de Ley".[13]

La citada LRJSP considera que estas Autoridades son entidades que integran el sector público institucional estatal, con funciones "de regulación o supervisión de carácter externo sobre un determinado sector o actividad económica",[14] "con independencia de cualquier interés empresarial o comercial".[15]

Este tipo de Autoridades, como establece la propia LRJSP, se van a regir por su Ley de creación, que deberá ser una norma con rango de Ley, por sus Estatutos y por la legislación específica del ámbito sometido a su supervisión, y con carácter supletorio, por lo previsto en la "Ley 47/2003, de 26 de noviembre, el Real Decreto Legislativo 3/2011, de 14 de noviembre, la Ley 33/2003, de 3 de noviembre, así como el resto de las normas de Derecho administrativo general y especial que le sea de aplicación".[16] Lo que implicará el sometimiento, para lo que aquí nos interesa, a la Ley 19/2013, de Transparencia, Acceso a la Información pública y buen Gobierno (LTAIBG).

2.1.1.- Objetivo: la protección de los derechos fundamentales

Las Administraciones públicas independientes surgen, como vemos, para regular o supervisar un determinado sector, afectando, para el caso que aquí nos ocupa, al derecho fundamental a la protección de datos personales.

Así las cosas, vemos que, en términos generales, los argumentos esgrimidos para justificar la creación de estas Autoridades han sido principalmente tres: la necesidad de establecer un mecanismo preventivo, la especialización técnica de las mismas, y, la independencia en el ejercicio de la tarea que tienen atribuida.

En primer lugar, este tipo de Autoridades se crean con la finalidad de prevenir la violación de los derechos de los individuos respecto del tratamiento de sus datos personales. Como ya sabemos, ante la lesión de un derecho, el ciudadano puede acudir a la vía jurisdiccional para la reparación del daño sufrido pero, en muchas ocasiones, el daño ocasionado tiene difícil reparación, por lo que se hacen necesarios mecanismos que eviten que se produzca la lesión del derecho. No podemos olvidar que las Autoridades de control "son el primer punto de contacto

[13] Art. 109.1 LRJSP.

[14] Vid. art. 84.1.b) y Apdo. V Exposición de Motivos LRJSP.

[15] Vid. art. 109.2 LRJSP.

[16] Art. 110.1 LRJSP.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

para los interesados en los casos de violación de la privacidad".[17] Esto es particularmente evidente en el campo de la protección de los datos personales, ya que frente a las amplias posibilidades que ofrecen las técnicas informáticas, la vía jurisdiccional posterior resulta insuficiente y poco adecuada. Así, por ejemplo, los tratamientos de datos que las Leyes consideren más peligrosos para los derechos y libertades de los interesados deben notificarse, por el responsable del tratamiento, a la Autoridad de protección de datos, que "controlará" dicho tratamiento.[18] El problema, sin embargo, es que, en definitiva, son los Estados miembros los que tienen que "implantar" este tipo de control previo en sus respectivos ordenamientos jurídicos, precisando los supuestos en los que es necesario.

En segundo lugar, otro de los motivos argumentados para crear este tipo de Autoridades es el de su especialización técnica. Se trata de un campo en el que es necesaria una cualificación y especialización técnica específica en la materia. Por eso, se ha argumentado que es conveniente que este tipo de Autoridades se componga de "especialistas" o "expertos" en la materia de la que se van a ocupar (Salvador Martínez, 2002: 348).

Y, en tercer lugar, aunque el motivo más importante que justifica la necesidad de crear estas Autoridades nacionales de protección de datos es la necesidad de crear un órgano independiente, que actúe libre de órdenes e instrucciones, en su labor de garantía del derecho a la protección de datos personales, sin estar movido por ningún tipo de interés político o económico. En este sentido destaca el objetivo de la "neutralidad política", mediante el que se explica la necesidad de que ciertas actividades se ejerzan al margen de las "luchas de partidos", y, más concretamente, de los órganos del Estado en los que tiene lugar la lucha política. Se ha afirmado así que la protección de ciertos derechos no puede dejarse en manos de órganos políticos del Estado, pues es frente a ellos, aunque no sólo, frente a quienes se quieren garantizar (Salvador Martínez, 2002: 344-348). Asimismo, hoy en día se hace imprescindible la existencia de Autoridades de control independiente que supongan un freno a los llamados gigantes tecnológicos del sector privado ante la evidencia de que los mismos están interfiriendo en nuestros derechos fundamentales en el proceso de digitalización que vivimos.

Aunque no existe una fórmula general que garantice la independencia, existen ciertos elementos organizativos que contribuyen a ella, como son, la composición de la Autoridad, el método de elección de sus miembros, la duración del ejercicio de

[17] Como se deriva del art. 13.2.d) RGPD. Vid. Agencia de los Derechos Fundamentales de la Unión Europea / Consejo de Europa / Supervisor Europeo de Protección de Datos, *Manual de legislación europea en materia de protección de datos*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2019, p. 215.

[18] Al respecto, vid. Considerandos 84, 94 y 96, y art. 36 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

su cargo y la forma de cesar en el mismo, la independencia económica y la independencia de órdenes o instrucciones. Y todo ello, para el caso que aquí nos ocupa, se verá garantizado si se cumplen unas reglas mínimas de transparencia, como luego veremos.

En este sentido, las normas sobre protección de datos establecen las características generales que deben cumplir este tipo de Autoridades, exigiéndolas ese carácter "independiente". Y son las normas de transparencia las que marcarán las pautas para lograr una más eficaz Administración pública. Se hace necesario conocer la organización y funcionamiento de estas Autoridades para luego analizar sus obligaciones de transparencia y comprobar su grado de cumplimiento.

2.1.2.- Las Autoridades de control en España

A nivel nacional, son múltiples y variados los ejemplos de Autoridades administrativas independientes creadas con la finalidad de controlar o regular un sector específico. Así, podemos citar, por ejemplo, la Comisión Nacional del Mercado de Valores, el Banco de España, la Comisión Nacional de los Mercados y la Competencia, el Consejo de Seguridad Nuclear y el Fondo de Reestructuración Ordenada Bancaria y, para lo que aquí interesa, la Agencia Española de Protección de Datos y el Consejo de Transparencia y Bueno Gobierno (y sus homólogos/as autonómicos/as).

Para la creación de este tipo de Autoridades en el terreno de la protección de datos a nivel nacional, en primer lugar, se tuvo en cuenta lo establecido en la normativa internacional y europea sobre la materia que vincula a nuestro Estado, a saber y como ya hemos dicho: el citado Convenio 108 del Consejo de Europa y la derogada Directiva 95/46/CE sobre Protección de Datos, actualmente el RGPD, que ha concretado los criterios establecidos en dichas normas. Como se puede ver, en Europa se ha optado, claramente, por la creación de un órgano especializado para la garantía del derecho a la protección de los datos personales.

En segundo lugar, el legislador español, de acuerdo con las normas antes mencionadas, entendió que, debido a las amplias posibilidades de lesión que ofrece, actualmente, la informática, era preciso crear un órgano independiente (Salvador

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Martínez, 2002: 266-267),[19] especializado en la materia, que respondiera de forma rápida y que actuara de forma preventiva (Salvador Martínez, 2002: 270).[20] En un principio se planteó la posibilidad de que fuera el Defensor del Pueblo el encargado de la protección de datos personales, aunque esta idea fue desechada por la posible desvirtuación que se produciría de la institución del Defensor del Pueblo, y se decidió crear un organismo específico: la AEPD.[21]

En nuestro ordenamiento jurídico, el Tribunal Constitucional se ha pronunciado sobre la necesidad de crear este tipo de Autoridades de protección de datos, en concreto de la citada AEPD. De acuerdo con el Tribunal Constitucional la creación de esta "Autoridad independiente" se deduce, por un lado, de la necesidad de una respuesta rápida, especializada técnicamente y que actúe de forma preventiva, pues, frente a las amplias posibilidades informáticas, la vía jurisdiccional resulta insuficiente e inadecuada para proteger los datos personales; y, por otro lado, de la necesidad de crear un órgano de control independiente del Gobierno, pues la Administración también debe cumplir las normas de protección de datos y queda sometida a control (Salvador Martínez, 2002: 270-271; y Sala Arquer, 1984: 426)[22]. El Tribunal Constitucional, por su parte, así lo ha reconocido, y ha mantenido que "la creación de dicho ente y las funciones atribuidas al mismo permiten garantizar el ejercicio por los ciudadanos del haz de facultades que integran el contenido del derecho fundamental a la protección de datos" (Salvador Martínez, 2002: 271).[23]

La cuestión, llegados a este punto es que, a pesar de tener las ideas claras de por qué surgen estas Autoridades, y cómo deben ser y actuar para dar sentido a su creación, el margen de actuación de los Estados en su diseño genera alguna dificultad. El RGPD, a pesar de ser una norma de aplicación directa —que deja menos

[19] Sobre la necesidad de crear una institución independiente que garantizara el derecho a la protección de datos, conviene recordar que la doctrina no ha dudado en afirmar que para el ejercicio de determinadas funciones cuya finalidad es la garantía de los derechos fundamentales la neutralidad e independencia vienen exigidas incluso constitucionalmente, pero que la CE no exige que se cree una "autoridad independiente" para el ejercicio de todas aquellas funciones relacionadas con un derecho fundamental. Es un problema de interpretación constitucional de los derechos fundamentales. Sobre la naturaleza constitucional de la Agencia, vid. Diario de Sesiones del Congreso de los Diputados, nº 744, VI Legislatura, de 15 de septiembre de 1999, p. 21877.

[20] Así lo reconoce también la STC 290/2000.

[21] El ampliar el campo de actuación del Defensor a los sujetos privados hubiera significado desnaturalizar la institución del Defensor del Pueblo, puesto que la Constitución, en su art. 54, y la LO 3/1981 del Defensor del Pueblo en su art. 1, le encomiendan al mismo la defensa de los derechos del Título I CE sólo respecto de la actuación de la Administración Pública.

[22] Vid. STC 290/2000, FJ 9º.

[23] SSTC 254/1993 y 290/2000.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

margen de maniobra a los Estados, de lo que puede dejar una Directiva—, contiene cincuenta y seis remisiones o cláusulas abiertas y de especificación (Viguri Cordero, 2022: 248) -excesivas, en nuestra opinión- a completar por los Estados. Esta técnica, más allá de la crítica de la técnica legislativa empleada, sigue generando cierta falta de uniformidad, desajustes y distorsión del mercado único digital entre los Estados miembros de la Unión Europea (García Mahamut, 2019: 101-103 y 107-110; y López Calvo, 2017: 53). Entre las citadas remisiones o cláusulas abiertas contenidas en el RGPD se encuentran las contenidas en los artículos citados que regulan las Autoridades de control.

Así, la consecuencia será, como ha quedado dicho, que las clasificaciones realizadas de dichas Autoridades son muy variadas: en función de su composición, ya que algunas son órganos colegiados y otras órganos unipersonales; en función de su grado de independencia funcional, dependiendo de si ejercen sus funciones dentro de la estructura de algún otro órgano administrativo o no; y en función de las competencias de la Autoridad (Rebollo Delgado, 2004: 167-169). Nosotros nos vamos a centrar aquí en las Autoridades de control creadas en España, tomando como modelo el marco previsto en la AEPD.

En España, dando cumplimiento a lo previsto en el art. 18.4 CE, la norma que se ha encargado de completar lo previsto en el RGPD y adaptarlo a nuestro Estado es la ya citada LOPDGDD, que regula la creación de las Autoridades de control en su Título VII (arts. 44 a 62), siendo su Estatuto aprobado por Real Decreto 389/2021 (EAEPD).[24] No nos detendremos aquí en la también citada LO 7/2021 porque la misma también reconoce como Autoridades de control a la AEPD y las Autonómicas equivalentes.[25] A nivel autonómico -teniendo en cuenta que el RGPD respeta "la arquitectura constitucional de cada Estado miembro" (Troncoso Reigada, 2016: 483-484)-,[26] y debido a la habilitación contenida en la actual LOPDGDD, como en las anteriores normas sobre protección de datos para que las Comunidades Autónomas regularan la materia, algunas Comunidades Autónomas crearon un "órgano de

[24] Tal y como prevé el art. 45.2 LOPDGDD. El Decreto 389/2021 vino a derogar el anterior EAEPD, aprobado por RD 428/1993 en cumplimiento de lo dispuesto en desarrollo de la LO 5/1992 de Tratamiento Automatizado de Datos Personales (la conocida como LORTAD).

[25] Lo hace en su Cap. VI, arts. 48 a 51 LO 7/2021.

[26] Art. 117 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

control" (Troncoso Reigada, 2005: 116 y 127-128).[27] Todo esto se traduce que en nuestro caso tendremos una Agencia Española de Protección de Datos (AEPD) a nivel nacional y tres Autoridades autonómicas de protección de datos: catalana, vasca y andaluza (Soriano Moreno, 2019: 272-278).[28]

Así las cosas, nos vamos a referir en este trabajo a las Autoridades autonómicas existentes con el fin de comprobar el cumplimiento de sus obligaciones de transparencia. Pero antes debemos conocer cómo surgieron y las normas que las regulan y desarrollan y si las mismas contienen alguna exigencia de transparencia y comprobar su grado de cumplimiento.

La Autoridad Catalana de Protección de Datos (APDCAT) surge como respuesta a lo previsto en su Estatuto de Autonomía para garantizar el derecho fundamental a la

[27] En España, la LOPDGDD regula la figura de las Autoridades autonómicas de protección de datos en el Cap. II del Tít. VII (art. 57 a 62), debiendo recordarse aquí que sus funciones y potestades, que serán las previstas en el RGPD para las Autoridades de control, se ejercerán en el marco de la normativa autonómica y de los tratamientos sometidos a su competencia. Sin entrar en detalle sobre la polémica que surgió en su día, obre la distribución de competencias en materia de protección de datos personales, ya tuvo ocasión de pronunciarse el Tribunal Constitucional en su Sentencia 290/2000 al hilo de resolver si la AEPD o las Agencias autonómicas eran competente sobre el control de los denominados ficheros privados (en términos generales, los no gestionados por el sector público). El Tribunal Constitucional afirmó que debe ser la AEPD quien controle todos los ficheros privados, incluso los que radiquen en las Comunidades Autónomas, porque la creación de la AEPD responde no sólo al mandato constitucional del artículo 18.4 CE, sino a la garantía de un derecho fundamental, el derecho a la protección de datos personales y, porque es competencia del Estado, en base al artículo 149.1.1 CE, asegurar el respeto de los derechos fundamentales en todo el territorio nacional mediante el establecimiento de las condiciones básicas que hagan posible que el disfrute de tales derechos sea igual para todos los ciudadanos. En idéntico sentido la STC 76/1984 resolvió un recurso de inconstitucionalidad interpuesto por el Abogado del Estado contra el art. 3.1.a) de la Ley 11/1982, de 8 de octubre, de creación del Instituto Cartográfico de Cataluña. De acuerdo con el TC, la actividad cartográfica tiene un carácter instrumental con relación a múltiples actividades de los particulares y respecto de numerosas actividades de las Administraciones públicas y el silencio de la CE y del Estatuto de Autonomía de Cataluña se aplica, no como una reserva tácita y residual de competencia estatal exclusiva del art. 149.3 CE, sino como un tácito reconocimiento de que la cartografía no es una materia sobre la que sólo se pueda actuar en virtud de normas de atribución de competencia, sino como una actividad técnica relacionada con competencias que, estas sí pueden pertenecer al Estado o a una Comunidad Autónoma.

[28] No podemos olvidar que en Madrid, la Ley 13/1995 de regulación del uso de la informática en el tratamiento de los datos personales por parte de la Comunidad de Madrid provocaron la creación de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), aunque dicha Agencia fue suprimida por Ley 8/2012 de Medidas Fiscales y Administrativas de la Comunidad Autónoma Madrileña.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

protección de datos.[29] Fue creada inicialmente por la Ley 5/2002, en virtud de la cual se aprobó su Estatuto por Decreto 48/2003. Debemos señalar aquí que el Estatuto de Autonomía catalán de 2006 reforzó la independencia de la Autoridad al establecer su designación parlamentaria, Estos cambios y la necesidad de adaptar la APDCAT a los cambios tecnológicos de los últimos años y su cambio de denominación de Agencia por la de Autoridad con el fin de no confundirla con las agencias o entidades de carácter instrumental, provocaron la aprobación de la Ley 32/2010 de creación de la Autoridad Catalana de Protección de Datos.

Por su parte, en el País Vasco, se creó la Agencia Vasca de Protección de Datos (AVPD) mediante la Ley 2/2004, por la que se regulan los Ficheros de Datos de Carácter Personal de Titularidad Pública. Su Estatuto fue aprobado al año siguiente mediante Decreto 309/2005. Si bien esta norma ha modificado su estructura orgánica en diversas ocasiones (como lo ha hecho mediante Resolución de 29 de marzo de 2023), su forma de elección y nombramiento no parecen adecuarse a lo exigido por el RGPD o al modelo seguido por la AEPD, a pesar de que en diciembre de 2022 se anunciara que se reformaría la normativa de protección de datos para adaptarla a la normativa europea.[30]

Por último, el Consejo de Transparencia y Protección de Datos de Andalucía (CTPD) se creó por la Ley 1/2014 de Transparencia Pública de Andalucía,[31] y aprobó su Estatuto mediante Decreto 434/2015.

Debemos criticar aquí que, a 5 años de la entrada en aplicación del RGPD, el 25 de mayo de 2018 -y de 7 de su entrada en vigor en 2016-, y de otros tantos años de la entrada en vigor de nuestra LOPDGDD el 6 de diciembre de 2018, las normas autonómicas que regulan la materia siguen sin actualizar y sin adaptarse al RGPD -por mucho anuncio que hayan hecho-, habiendo pasado ya un periodo más que prudencial para adecuar sus procesos internos (Viguri Cordero, 2022: 244).

[29] Vid. art. 31 EA Cataluña (aprobado por LO 6/2006, de Reforma del Estatuto de Autonomía de Cataluña): "Artículo 31. Derecho a la protección de los datos personales. Todas las personas tienen derecho a la protección de los datos personales contenidos en los ficheros que son competencia de la Generalitat y el derecho a acceder a los mismos, a su examen y a obtener su corrección. Una autoridad independiente, designada por el Parlamento, debe velar por el respeto de estos derechos en los términos que establecen las leyes".

[30] Vid. "Euskadi adaptará su normativa de protección de datos al Reglamento Europeo", en *Noticias de Guipuzcoa*, de 21 de diciembre de 2022.

[31] Arts. 43 a 49 Ley andaluza 1/2014.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

2.2.- Organización, composición y funcionamiento

Con carácter general, el RGPD reconoce la autonomía personal,[32] presupuestaria y financiera de las Autoridades de control,[33] pudiendo ser controlada incluso judicialmente.[34] Es evidente que si las mismas dependen económicamente de quienes las nombran, la independencia es más que cuestionable. De ahí que el RGPD se refiera a la necesidad de que las mismas dispongan de "un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional"[35], siendo los Estados los que decidirán en último término este extremo.

En España nuestra LOPDGDD reconoce dicha autonomía financiera y presupuestaria, integrándose su presupuesto de forma independiente en los Presupuestos Generales del Estado, siendo de destacar que los ingresos que la Autoridad recaude, pasarán a formar parte de sus reservas con el fin de garantizar su independencia. Por su parte, las normas autonómicas también reconocen dicha independencia.[36]

Con el fin de hacer frente a las funciones asignadas y ser eficaz en la garantía del derecho a la protección de datos, el RGPD exige que las Autoridades de control cuenten con "recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios" para cumplir con la función que tienen asignada[37].

Nos detenemos en este punto porque es en relación con su personal, concretamente con sus órganos de dirección y la forma de nombrarles lo que más polémica ha generado (con carácter general, vid. el excelente artículo de García Mahamut, 2023). Sobre todo, a nivel estatal. Y será aquí donde encontraremos la única referencia a la exigencia de transparencia.

De forma novedosa el RGPD regula los requisitos para ser nombrado miembro de la Autoridad de control, a saber: poseer la titulación, la experiencia y las aptitudes, en

[32] Así, cada Autoridad de control pueda elegir a su propio personal (art. 52.5 RGPD); y, sobre esta cuestión, con el fin de garantizar la independencia de la institución, vid. STJUE de 16 de octubre de 2012, Comisión europea contra Austria (C-614-/10), §§ 59 y 63, donde el TJUE dejó claro que el hecho de que los poderes públicos (en este caso era la Cancillería federal austriaca) facilitase personal a la Autoridad de control suponía una lesión del requisito de independencia.

[33] Art. 52.6 RGPD.

[34] Art. 52.6 RGPD y Considerando 118 RGPD.

[35] Art. 52.6 RGPD.

[36] Art. 52.4 RGPD y Considerando 120 RGPD. A su vez, vid. arts. 2 y 4 Ley catalana 32/2010; arts. 10-13 Ley vasca 2/2004; y arts. 43-44 Ley andaluza 1/2014.

[37] Vid. art. 52.4 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes (art. 53.2 RGPD), más allá de reunir unas "cualificaciones y condiciones de idoneidad necesarias",[38] aunque bien es cierto el amplio margen de discrecionalidad que reúne ese carácter de "idóneo".

El RGPD dispone que el nombramiento de los miembros de la Autoridad de control se realice "mediante un procedimiento transparente", dando varias posibilidades: por el Parlamento, por el Gobierno, por el Jefe del Estado o por un organismo independiente encargado de dicho nombramiento.[39] Lo que en España, a nivel nacional, se ha traducido en un cambio radical -respecto de lo previsto en la normativa anterior- en la forma de elección de la Presidencia, y ahora también Adjunto/a a la Presidencia, de la AEPD.[40] A nivel autonómico, las Autoridades catalana y andaluza ya prevén un sistema en el que intervienen los respectivos parlamentos autonómicos, lo que no se produce en el caso de la Autoridad vasca, que, como hemos dicho, sigue sin adecuarse al procedimiento previsto en el RGPD o en la LOPDGDD.

El RGPD introduce como novedad que el tiempo mínimo del mandato de los miembros de las Autoridades de control nunca podrá ser inferior a cuatro años,[41] aunque sin dejarlo cerrado (como el hecho de su carácter renovable o del número de veces que podrá renovarse),[42] con el fin de que no coincida con el de los órganos de los que proviene el nombramiento.[43]

En este sentido, la LOPDGDD estable un mandato de 5 años para la Presidencia y Adjunto/a de la AEPD, que podrá renovarse por otro periodo de igual duración,[44] tal y como sucede, por ejemplo, con el Defensor del Pueblo. Asimismo, mientras dure el mandato, los miembros de las Autoridades de control son "inamovibles". La inamovilidad es una forma más de garantizar la independencia tanto de los

[38] Art. 54.1.b) RGPD.

[39] Art. 53 RGPD.

[40] Art. 48 LOPDGDD.

[41] Art. 54.1.d) RGPD.

[42] Art. 54.1.e) RGPD.

[43] Recoge así el pronunciamiento del TJUE sobre el mandato y la duración del mismo en el asunto Comisión europea contra Hungría, de 8 de abril de 2014 (§§ 50 y 67), donde se concluyó que, con el fin de garantizar la independencia de las Autoridades de control, los Estados miembros debían respetar la duración del mandato de la Autoridad "hasta que llegue al término inicialmente previsto".

[44] Art. 48.5 LOPDGDD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

miembros como de la propia institución. El RGPD dispone que éstos "únicamente" podrán ser destituidos "en el caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones",[45] señalando igualmente que podrán terminar su mandato, cesarán, por terminación del mismo, por dimisión o por jubilación obligatoria.[46] En la LOPDGDD se establece también su inamovilidad excepto en una serie de casos tasados en los que la separación además de ser acordada por Consejo de Ministros deberá contar con la misma ratificación del Congreso que para su nombramiento.[47] Este modelo no se reproduce a nivel autonómico ni en lo que a la duración del mandado se refiere (por ejemplo, en el País vasco, que dispone un mandato de 4 años) ni a la duración del mandato (por ejemplo, en Cataluña no tendrá carácter renovable).

Al margen de estas cuestiones, y sobre el procedimiento de nombramiento, a nivel autonómico, aunque el RGPD habla de un proceso transparente -lo que recordamos que no hace nuestra LOPDGDD-, la Ley catalana de creación de la APDCAT no menciona en ningún momento la referencia a la transparencia del proceso de selección de su Director/a.[48] lo que tampoco menciona ni detalla su Estatuto. Por su parte, la Ley vasca de creación de la AVPD tampoco menciona la palabra transparencia a lo largo de su articulado, siendo el nombramiento de su Director el que menos se adecúa a las exigencias de transparencia reconocidas actualmente por el RGPD -a pesar del anuncio de su adecuación a finales de 2022-, al ser nombrado directamente por Decreto del Gobierno y por un periodo de 4 años.[49] Tampoco su Estatuto menciona la palabra transparencia a lo largo de su articulado omitiendo toda referencia al proceso de nombramiento de su Director. En Andalucía a pesar de que es la Ley de Transparencia la que regula la materia, curiosamente tampoco se detalla el procedimiento de selección de la Dirección del Consejo, que será desarrollado por su Estatuto, pero que tampoco hace referencia a los principios de transparencia en el proceso más allá de indicar que se seguirá el "procedimiento que determine la Cámara".[50]

[45] Art. .53.4 RGPD.

[46] Art. 53.3 RGPD. Sobre la importancia de recoger las causas de cese o de duración en el ejercicio de sus funciones, más allá de la STJUE de 8 de abril de 2014, Comisión europea contra Hungría (C-288/12, §§ 50 y 67), vid. el interesante argumento del Informe explicativo del Convenio 108+, apdo. 129.

[47] Art. 48.5 LOPDGDD.

[48] Art. 7 Ley catalana 32/2010.

[49] Art. 15 Ley vasca 2/2004.

[50] Art. 47 Ley andaluza 1/2014; y art. 11 Decreto andaluz 434/2015.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

No obstante, como hemos señalado, ha sido el procedimiento de selección de la Presidencia y Adjunto/a a la AEPD lo que más polémica ha causado (García Mahamut, 2023). Y no solo por el cambio radical experimentado en el procedimiento, sino por la evidente intervención política en el proceso de elección más allá del procedimiento legalmente previsto, que saltó a los medios de comunicación y llegó incluso a los Tribunales. A nivel nacional, pasamos de un Director/a a una Presidencia, con sus respectivas funciones, y a la aparición de un Adjunto/a (Arenas Ramiro, 2019: 235-240), que tendrá en ciertos puntos un régimen similar a la Presidencia, siendo ambos considerados Altos cargos de la Administración General del Estado.[51]

Por último, queríamos señalar que nuestra LOPDGDD prevé, junto a la Presidencia y Adjunto/a, la existencia de un órgano de asesoramiento, que es el Consejo Consultivo. Si bien es cierto que esta figura ya existía con la anterior normativa nacional, destaca ahora la ampliación del número de sus miembros, su variada composición y la forma de elección de sus miembros, que refleja una pluralidad de opiniones que pueden fomentar un rico debate democrático con profesionales de la privacidad, la seguridad o la transparencia (Martínez Martínez, 2019: 17).[52] Además, debemos destacar igualmente el hecho de que sus miembros deben tener la consideración de "expertos", para lo que se exige acreditar "conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico".[53]

A nivel autonómico también existe este Consejo Consultivo, aunque con diferente denominación y composición. En Cataluña se denomina Consejo Asesor de Protección de Datos, en el País Vasco Consejo Consultivo, y en Andalucía, Comisión Consultiva de la Transparencia y la Protección de Datos.[54]

2.3.- Competencias y funciones

El RGPD se ha encargado de fortalecer a las Autoridades de control en todas sus funciones y competencias, a diferencia de la escasa mención que hacía la Directiva 95/46/CE al respecto.[55] El RGPD ha reforzado y concretado los poderes de las Autoridades de control, especialmente los relacionados con su potestad investigadora y coercitiva o sancionadora, pero desde el requisito de la

[51] Art. 48.2 LOPDGDD.

[52] Art. 49.1 LOPDGDD.

[53] Art. 49.2 LOPDGDD.

[54] Art. 9 Ley catalana 32/2010; art. 16 Ley vasca 2/2004; y art. 49 Ley andaluza 1/2014.

[55] Art. 28.3 Directiva 95/46/CE (derogada).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

independencia. De esta forma, se han hecho más eficaces sus labores de supervisión del cumplimiento de la normativa de protección de datos.

De ahí la importancia de reforzar la independencia en el ejercicio de sus funciones y competencias, garantizándose así una objetividad plena en sus decisiones.[56] Y, por lo tanto, la importancia de reforzar que estas funciones se ejerzan con total transparencia. Debemos añadir que esta exigencia de independencia se vería vacía de contenido si la misma no pudiera ser probada y controlada. De ahí la exigencia no solo del control de las Autoridades, sino la exigencia de transparencia en su funcionamiento, lo que se va a reflejar en sus Informes de actividad y, en el caso español, en la publicidad también de las resoluciones de la Presidencia.[57]

A nivel nacional, la LOPDGDD recoge las funciones y potestades de la AEPD en su artículo 47, con expresa mención a los artículos 57 y 58 RGPD (Arenas Ramiro, 2019: 229-234.).

Sin detenernos en los poderes y funciones llevados a cabo por las Autoridades de control, debemos dejar señalado que las Autoridades de control, más allá de velar por el correcto cumplimiento de la normativa de protección de datos[58], todas tienen reservadas una serie de competencias mínimas recogidas en el RGPD (y que pueden ser ampliadas por los Estados),[59] a saber: poderes de investigación,[60] poderes correctivos, y poderes de autorización y consultivos.[61] Y tienen también toda una

[56] Art. 52.1 RGPD y como también exige el art. 15.5 del citado Convenio 108 +.

[57] Art. 59 RGPD y art. 50 LOPDGDD.

[58] Lo que en la AEPD se traduce también en la potestad de elaborar Circulares. Hasta el momento: la Circular 1/2019, de 7 de marzo, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, del Régimen Electoral General; y la Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

[59] Todo ello con el fin de garantizar una supervisión y ejecución coherente en toda la Unión Europea. Vid. Considerando 129 RGPD.

[60] Así, el TJUE ha concluido que este poder de investigación debe entenderse en un sentido amplio con el fin de garantizar una protección eficaz del derecho a la protección de datos, permitiendo que las Autoridades de control puedan tomar y llevar a cabo las medidas necesarias. Vid. STJUE de 6 de octubre de 2015, Maximiliam Schrems contra Data Protection Commissioner (C-362-14, §§ 26-36 y 40-41). En este caso, el TJUE consideró que las Autoridades de control podían impedir la transferencia de datos personales a Estados Unidos, aunque existiera una decisión de idoneidad si existían pruebas razonables de que en Estados Unidos ya no estaba garantizado el derecho.

[61] Art. 58 RGPD. Vid., también, Instrucción 1/2021, de la AEPD, por la que se establecen directrices sobre la función consultiva de la Agencia.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

serie de funciones de supervisión proactiva y preventiva que pueden englobarse en su potestad investigadora.[62] Así pueden investigar las operaciones de tratamiento e intervenir en caso necesario,[63] y paralizar tratamientos si no lo ven suficientemente transparente, como ha sucedido y está sucediendo con el caso de la herramienta de Inteligencia Artificial ChatGPT.[64] No obstante, queremos dejar señalado igualmente que es en relación con sus poderes correctivos, en el terreno sancionador donde se ha encontrado una mayor divergencia a la hora de aplicar la normativa de protección de datos entre los Estados miembros (Viguri Cordero, 2022)[65]. La LOPDGDD refuerza el marco procedimental sancionador e introduce en el procedimiento a la figura del Delegado/a de Protección de Datos (Martínez Martínez, 2019: 17).

Sin adentrarnos en el funcionamiento de los mecanismos de cooperación y coherencia que el RGPD regula en su Capítulo VII (arts. 60 a 68) (Viguri Cordero, 2015: 739-769; e Irurzun Montoro, 2016: 513-526; López Calvo, 2018: 609-632; y Viguri Cordero, 2021: 167), para lo que aquí nos interesa, por lo que luego analizaremos respecto de las obligaciones de transparencia, debemos recordar que con estos mecanismos, el RGPD detalla la competencia y cooperación de las Autoridades de control, con especial referencia a los casos de tratamientos de datos personales transfronterizos, esto es, en aquellos tratamientos en los que habrá más de una Autoridad de control implicada, bien porque el responsable del tratamiento tenga establecimientos en más de un Estado, o bien porque el tratamiento afecta sustancialmente a los interesados en más de un Estado miembro. En estos casos se hace indispensable, hoy más que nunca, el intercambio de información y el cumplir con la homogeneización normativa que persigue el RGPD (García Mahamut, 2019: 97). Y aquí es donde se hace indispensable tener en cuenta la estricta aplicación de la transparencia con el fin de reforzar la seguridad jurídica, a la vez que las decisiones se adoptan con una mayor rapidez, evitando pronunciamientos contradictorios.

2.3.- Obligaciones de transparencia de las Autoridades de control

El objetivo de las normas de transparencia en la Administración pública es acercar la Administración al ciudadano, darles a conocer el funcionamiento de la institución y la toma de decisiones, garantizándose así la participación de los ciudadanos en los

[62] Art. 57 RGPD.

[63] Art. 58 RGPD.

[64] Más allá de las decisiones del Garante italiano de suspender su uso en Italia, vid. AEPD, Nota de prensa "La AEPD inicia de oficio actuaciones de investigación a OpenAI propietaria de ChatGPT", de 13 de abril de 2023.

[65] De ahí, por ejemplo, la aprobación de la Instrucción 1/2023, de la AEPD, sobre gestión de aplazamientos y fraccionamientos de pago.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

asuntos públicos mediante un mejor conocimiento de la acción del Estado, fortaleciendo el principio democrático.

De este modo, con carácter general, habrá que entender que, cuanto más transparente sea una Administración pública, se contribuye mejor a que los ciudadanos puedan conocer los criterios de organización y funcionamiento de las instituciones, así como su financiación y lo que hacen con los presupuestos asignados.

Cuando esta exigencia de transparencia se predica de Autoridades administrativas independientes, como son las Autoridades de protección de datos, dicha exigencia debe ser aún mayor pues estamos ante Autoridades administrativas que están llevando a cabo funciones cuasilegislativas —al tener capacidad normativa— y cuasijudiciales —interpretan y deciden sobre derechos fundamentales con su potestad de resolución administrativa—.

Así las cosas, si bien es cierto que su principal característica es su "total independencia"[66] -cualidad ésta que se ha recogido no sólo por diferentes textos normativos más allá del RGPD,[67] sino que se ha puesto de manifiesto por el TJUE en más de una ocasión-[68], la independencia sólo se puede entender en el marco de la transparencia, de una organización y un funcionamiento transparentes. Será la

[66] STJUE de 9 de marzo de 2010, Comisión europea contra Alemania (C-518/07, § 27). En este asunto, el TJUE consideró que someter la actuación de las Autoridades de control a vigilancia estatal constituía una violación del requisito de independencia. La "total independencia" debía entenderse, a juicio del TJUE como la independencia del SEPD, que no pueda solicitar ni recibir instrucción de nadie. Y así, concluyó que "en el ejercicio de sus funciones, las Autoridades de control deben actuar con objetividad e imparcialidad y, para ello, han de estar a resguardo de toda influencia externa, incluida la ejercida directa o indirectamente por las autoridades públicas" (§ 25). Todas estas cuestiones tienen su reflejo ahora en el art. 52 RGPD, que establece los requisitos mínimos para garantizar esa independencia total.

[67] Considerandos 92 y 117 RGPD. En la Unión Europea dicha exigencia la encontramos en el art. 8.3 CDFUE y en el art. 16.2 TFUE, que vienen a considerar que el respeto a las normas de protección de datos personales debe estar sujeto al control de una Autoridad independiente. A nivel internacional dicha exigencia se reconoce en el ahora art. 15.5 Convenio 108 + (modificación del Convenio 108, de 1981, aprobada el 10 de octubre de 2018; y ratificado por España el 28 de enero de 2021), así como, de forma más detallada en el Protocolo adicional al Convenio 108 sobre las autoridades de supervisión y los flujos transfronterizos de datos (STE nº 181), de 8 de noviembre de 2001.

[68] Citamos aquí la STJUE de 9 de marzo de 2010, Comisión europea contra Alemania (C-518/07, §§ 23 y 25); la STJUE de 16 de octubre de 2012, Comisión europea contra Austria (C-614/10, § 37); la STJUE de 8 de abril de 2014, Comisión europea contra Hungría (C-288/12, §§ 47-62), donde se condenó al país por cesar antes de tiempo a los dirigentes de dicha Autoridad; y la conocida STJUE de 6 de octubre de 2015, Maximilliam Schrems contra Data Protection Commissioner (C-362/14, §§ 38-66).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

transparencia la condición necesaria para garantizar la necesaria independencia de estas entidades.

El rasgo de independencia que caracteriza a estas Autoridades de control es una de las características más estudiadas y que más dificultades ha planteado, y aunque nos vamos a centrar en este apartado en analizar cuáles son las exigencias de transparencia previstas tanto en la legislación sobre transparencia como en las normas sobre protección de datos vigentes en España, entendemos que el cumplimiento de las obligaciones de transparencia contribuirán a reforzar la independencia de las mismas, como tendremos oportunidad de ver.

Esta exigencia obedece, entre otros motivos y obligaciones legales, al cumplimiento del principio de buena Administración previsto en el art. 103.1 de nuestro texto constitucional (aunque también lo podemos entender vinculado al derecho de acceso a la información pública previsto en el art. 105 CE). Para que la sociedad pueda crearse una opinión pública debe controlar la actuación del poder y participar en su ejercicio y, para ello, es indispensable que la información sobre dicho poder sea transparente (Guichot Reina, 2017: 556). Asimismo, la transparencia es la esencia del principio democrático. No puede haber democracia sin transparencia porque la democracia implica no sólo participación, sino un control eficaz del poder, y sólo es posible controlar lo que se conoce (Guichot Reina, 2017: 556; Gutiérrez David, 2014: 187; y Blanes Climent, 2014: 154). En esta línea, es innegable que la transparencia tiene una connotación legitimadora en la conciencia de los ciudadanos, de ahí que el sistema sea más o menos democrático en función de la confianza que los ciudadanos tengan en dicho sistema. No debemos olvidar que no hay democracia sin control. De ahí que la transparencia no sea sólo en un requisito formal o "estético", sino de fondo, debiendo ser la información suministrada, entre otras cosas, como luego veremos, de calidad, comprensible y en un formato adecuado (Delgado Morales, 2017: 322).

En España, las obligaciones de transparencia, como ya ha quedado dicho, se desarrollan en la citada Ley 19/2013, de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTAIBG) que, con sus luces y sus sombras (Guichot, 2013), consolidó la transparencia como un principio informador y vertebrador de nuestro ordenamiento jurídico, provocando que muchas otras normas regularan, aunque

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

fuera de forma accesoria, la transparencia en la actuación de los poderes públicos,[69] e introdujeran una exigencia de transparencia en el funcionamiento de otros sujetos constitucionalmente reconocidos, como fue en el caso, por ejemplo, de los partidos políticos. La citada LTAIBG recoge un conjunto de obligaciones destinadas a incrementar y reforzar la transparencia en la actividad pública, lo que se conoce como transparencia activa o publicidad activa, a la vez que garantiza el acceso a la información, también conocido como publicidad pasiva o derecho de acceso, y establece una exigencia de responsabilidad para todos los sujetos que desarrollen actividades de relevancia pública.[70]

Tras la aprobación de la LTAIBG, las Comunidades Autónomas empezaron a aprobar sus Leyes de transparencia, siendo Andalucía la Comunidad pionera a nivel autonómico en 2014, y la Comunidad Autónoma Valenciana la última en modificar su normativa en 2022.[71] De la legislación autonómica existente debemos destacar que, a diferencia de la LTAIBG, las leyes autonómicas son mucho más precisas y desarrollan con más claridad aquellas cuestiones que la LTAIBG deja abiertas o no define como el propio concepto que luego explicaremos de lo que es la publicidad activa, esto es, la obligación de publicar información pública. De la misma forma, para lo que aquí nos interesa, las leyes autonómicas van a regular de una forma mucho más detallada un régimen sancionador mucho más concreto que el prácticamente inexistente recogido en la LTAIBG, incluyendo también de forma

[69] Así, por ejemplo, las Leyes 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC) y 40/2015, de Régimen Jurídico del Sector público (LRJSP). La Ley 39/2015 recoge la obligación de transparencia entre las normas generales de actuación de las Administraciones públicas como parte de los derechos de los ciudadanos en sus relaciones con la Administración (art. 13.d)), así como entre los principios de buena regulación (art. 129) y de ordenación del procedimiento (art. 71). Por su parte, la Ley 40/2015 se refiere a la transparencia como uno de los principios generales de actuación y funcionamiento del sector público (art. 3.1.c), del sector público institucional (art. 81) y de las sociedades mercantiles estatales (art. 112); además de incluirla como un principio esencial en el funcionamiento electrónico del sector público (art. 38.3 sobre la sede electrónica) y en la reutilización de los sistemas y aplicaciones o herramientas propiedad de la Administración (art. 157).

[70] Preámbulo LTAIBG.

[71] Al respecto, Ley andaluza 1/2014, de Transparencia Pública de Andalucía; y Ley valenciana 1/2022, de Transparencia y Buen Gobierno de la Comunitat Valenciana. En la actualidad, todas las Comunidades Autónomas tienen Leyes de transparencia y todas ellas incluyen en su título la palabra Transparencia excepto las Leyes de Extremadura, Islas Baleares, y País Vasco, que se refieren al buen Gobierno, al Gobierno abierto o a las Instituciones locales, respectivamente, regulando la transparencia en artículos, capítulos o títulos completos. Las dos Ciudades Autónomas, Ceuta y Melilla, no tienen Leyes de transparencia, pero mientras Melilla goza de un Reglamento de Transparencia y Acceso a la Información Pública, Ceuta se ha limitado a firmar con el CTBG un Convenio para la resolución de las reclamaciones en esta materia.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

específica sanciones para el caso de incumplimientos en materia de publicidad activa, como ocurre en los casos de la citada Ley de Andalucía, a la que luego nos referiremos. Nos detendremos sólo en lo previsto en las normas autonómicas donde existe una Autoridad de control en materia de protección de datos: Cataluña, País Vasco y Andalucía.

Como órgano de control, encargado de velar por su cumplimiento, la LTAIBG creó el Consejo de Transparencia y Buen Gobierno (CTBG)[72] como autoridad de control independiente encargada de supervisar y controlar la correcta aplicación de las obligaciones contenidas en la LTAIBG.[73]

A nivel autonómico la mitad de las Comunidades Autónomas han creado un Consejo de Transparencia u órgano equivalente, siendo el caso más modélico el del Andalucía con su Consejo de Transparencia y Protección de Datos de Andalucía. Modélico en tanto que, de forma novedosa en España, asume conjuntamente funciones de transparencia y protección de datos. Más allá de éste, o casos similares (como Aragón, Canarias, Comunidad Valenciana, Murcia, Navarra, País Vasco o la Comunidad de Madrid), el resto de Comunidades Autónomas han firmado Convenios con el CTBG para dar respuesta al ejercicio del derecho de acceso (como Asturias, Islas Baleares, Ceuta, Melilla, Cantabria, Extremadura o La Rioja), o han creado una Comisión independiente adscrita a la figura equivalente al Defensor del Pueblo, como es el caso de Castilla y León, que adscribe su Comisión al Procurador del Común, o Galicia, que lo adscribe al Valedor do Pobo. En Cataluña, además de contar con la Comisión de Garantía del Derecho de Acceso a la Información Pública, el Sindic de Greuges se va a encargar de vigilar el cumplimiento de la obligación de publicidad activa.

No corresponde aquí detenernos en analizar estas figuras más allá de la que se ha creado en Andalucía en cuanto a sus funciones como Autoridad de control en materia de protección de datos. Y, como pasa con las Autoridades de protección de datos, lo más destacable, si bien al margen de lo que las normas exigen sobre transparencia, será fijarnos en sus funciones,[74] y, más concretamente, en las funciones de control y en su capacidad sancionadora.[75]

Centrándonos en el caso del tratamiento de datos personales y de las Autoridades encargadas de su control, éstas serán autoridades administrativas independientes, tal y como hemos explicado. Así, la LOPDGDD nos dice que la AEPD "es una

[72] Tít. III LTAIBG (arts. 33 a 40).

[73] Art. 34 LTAIBG.

[74] Art. 38 LTAIBG.

[75] Art. 38.2 LTAIBG.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

autoridad administrativa independiente de ámbito estatal",[76] y remite a lo previsto para estas figuras a la Ley 40/2015 del Régimen del Sector Público (LRJSP) (Salvador Martínez, 2019: 222-224).[77] De la misma forma lo indican las normas que regulan la creación de las Autoridades de protección de datos autonómicas citadas.[78]

En ese sentido, en tanto que autoridades administrativas independientes de ámbito estatal, podemos entender que las mismas se encuentran incluidas dentro del ámbito subjetivo de aplicación de la LTAIBG, al indicar comprendidos en el mismo: "Los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad".[79] Si bien la LTAIBG no se refiere expresamente a las Autoridades administrativas independientes en la definición ofrecida (y mucho menos a las autonómicas), ha sido su órgano de control, el CTBG el que, en el año 2019, interpretó que las mismas deberían entenderse incluidas en dicha definición.[80]

El CTBG entiende que si bien la LTAIBG parece excluir de su ámbito de aplicación a las Autoridades administrativas independientes al no mencionarlas expresamente, dicha exclusión no tendría sentido, como tampoco lo tendría la exclusión de la Autoridades administrativas independientes autonómicas porque, entre otros motivos, la citada Ley no distingue entre ámbito estatal y autonómico. Si tenemos en cuenta, por ejemplo, que la Ley 9/2017, de Contratos del Sector público se aplicaba al ámbito contractual, no tendría sentido no hacerlo en relación con sus actuaciones en materia de publicidad activa o derecho de acceso a la información pública. Y en relación con Autoridades autonómicas, el CTBG añade que aunque las normas de la LRJSP que regulan las Autoridades administrativas independientes no tienen carácter básico y su incorporación dependa de la legislación autonómica, a falta de normativa autonómica que las reconozca así expresamente, o por aplicación supletoria de la estatal, las mismas deben entenderse sujetas a las obligaciones de transparencia.

---

[76] Art. 44 LOPDGDD.

[77] Arts. 109 y 110 LRJSP. La LOPDGDD se refiere expresamente al apartado 3 del art. 109. Vid. art. 44 LOPDGDD. Hasta la citada LRJSP, los organismos reguladores o supervisores aparecían mencionados solo en la Ley 2/2011, de Economía Sostenible con referencia a la Mejora del entorno económico.

[78] Vid. arts. 1 y 2 Ley catalana 32/2010; art. 10 Ley vasca 2/2004; y art. 43 Ley andaluza 1/2014.

[79] Art. 2.1.c) LTAIBG.

[80] Al respecto, vid. Criterio interpretativo 3/2019, del CTBG, sobre *Publicidad activa (2). Ámbito subjetivo*, de 20 de diciembre de 2019.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

3.1.- En las Leyes de transparencia

La LTAIBG establece un conjunto de obligaciones para las Administraciones públicas y otras instituciones y organismos, entre los que hemos dicho se encuentran las Autoridades de control en materia de protección de datos. Entre esas obligaciones podemos distinguir entre obligaciones de publicidad o transparencia activa y de transparencia pasiva o derecho de acceso a la información pública.[81]

Curiosamente, la LTAIBG no contiene una definición de lo que es la publicidad activa.[82] Es cierto que la misma se puede inferir del Preámbulo de la Ley y de sus preceptos, pero esta indeterminación ha sido aprovechada por algunas Comunidades Autónomas que sí que han incluido lo que debe entenderse por publicidad activa,[83] señalándose además de forma expresa que la misma es una "obligación".[84]

Conforme se deriva de la LTAIBG, las Autoridades de control, en tanto que sujetos obligados deberán hacer pública, en primer lugar, toda aquella información institucional, organizativa y de planificación de los mismos.[85] Esto implica, entre otras cosas, que las Autoridades de control deben hacer públicas no sólo las funciones que desarrollan y la normativa que les es aplicable, sino un organigrama actualizado, identificando a los responsables e incluyendo su perfil y su trayectoria profesional.

En segundo lugar, las Autoridades de control están obligadas a hacer pública, en concreto, su información económica, presupuestaria y estadística, y deberán publicar, como mínimo "la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria".[86] Entre esta información se incluyen

---

[81] El primer grupo de medidas o de "publicidad activa" está regulado principalmente en el Capítulo II del Título I titulado "Transparencia de la actividad pública"; y el segundo sobre "derecho de acceso a la información pública" aparece regulado en el Capítulo III del mismo Título I LTAIBG.

[82] Ha sido el CTBG el encargado de ofrecernos una definición en sus Criterios interpretativos. Al respecto, vid. Criterio Interpretativo 2/2019 sobre Publicidad activa (2). Concepto y Naturaleza, del CTBG, de 20 de diciembre de 2019.

[83] Así, por ejemplo, la Ley 1/2014, de Transparencia Pública de Andalucía en su art 2.b) señala que es "la obligación de las personas y entidades a las que hacen referencia los artículos 3 y 5 de hacer pública por propia iniciativa, en los términos previstos en la presente ley, la información pública de relevancia que garantice la transparencia de su actividad relacionada con el funcionamiento y control de su actuación pública".

[84] Así lo indica el CTBG en su Criterio Interpretativo 2/2019, de 20 de diciembre, sobre publicidad activa (1): concepto y naturaleza.

[85] Art. 6 LTAIBG.

[86] Art. 8 LTAIBG.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

contratos, convenios suscritos o encomiendas de gestión, así como subvenciones y ayudas públicas concedidas, los presupuestos, las cuentas anuales, así como los informes de auditoría de cuentas y de fiscalización, las retribuciones percibidas anualmente por los altos cargos y máximos responsables, así como las indemnizaciones percibidas con ocasión del abandono del cargo, las resoluciones relacionadas con causas de compatibilidad, las declaraciones anuales de bienes y actividades de los representantes locales, garantizándose la privacidad y seguridad de sus titulares, y la información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos prestados.

En relación con la información en materia económica y financiera, aunque no recogido expresamente en la LTAIBG, sino en la modificación que ésta introduce en la Ley 10/2010, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, se incluye dentro de la categoría de personas con responsabilidad pública a los sujetos que tengan la consideración de Altos cargos (tanto a nivel estatal como autonómico), lo que convierte a los cargos directivos de las Autoridades de control (Presidencia y Adjunto/a) en sujetos de las obligaciones correspondientes en materia de prevención del blanqueo de capitales.[87]

Toda esta información, conforme dispone la LTAIBG, será publicada en las sedes electrónicas o páginas web de los sujetos obligados. Es importante recordar aquí, dado que éste será uno de los problemas detectados y que tendrá consecuencias prácticas y de fondo, que la LTAIBG exige que dicha información debe publicarse "de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables".[88] Asimismo, la LTAIBG dispone que se establezcan los "mecanismos adecuados" para "facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización",[89] y exige que, para las personas con discapacidad se cumpla con el "principio de accesibilidad universal y diseño para todos".[90]

Como ya hemos señalado, la transparencia no puede ser sólo una cuestión "estética". Si se ofrece información, pero no se hace de la forma adecuada, no sirve para nada,

[87] Art. 14 Ley 10/2010, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, conforme a la modificación introducida por la Disp. Final Sexta.5 LTAIBG.

[88] Art. 5.4 LTAIBG. Debemos atender aquí a lo previsto en el ENI y a la Ley de reutilización Esquema Nacional de Interoperabilidad aprobado por el Real Decreto 4/2010, de 8 de enero, así como las normas técnicas de interoperabilidad. Reutilización: fomentando que la información sea publicada en formatos que permitan su reutilización, de acuerdo con lo previsto en la Ley 37/2007, de 16 de noviembre sobre reutilización de la información del sector público y en su normativa de desarrollo.

[89] Art. 5.4 LTAIBG.

[90] Vid. art. 5.5 LTAIBG y Preámbulo LTAIBG.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

y no cumple con el objetivo que la LTAIBG quiere conseguir: una mejor fiscalización de la actividad pública que contribuya a la necesaria regeneración democrática y, con ello, logre promover la eficiencia y eficacia del Estado, favoreciendo también el crecimiento económico. La transparencia en el funcionamiento y actuación de las Autoridades de control sólo será útil si la información a la que se accede, o que se publica, permite no sólo conocer, sino también controlar.

No es esta una cuestión baladí. Y no sólo porque estemos ante un incumplimiento de una obligación legal, sino porque su falta de cumplimiento, es decir, publicar información no accesible o no comprensible tiene las mismas consecuencias que no publicar nada, esto es, la vuelta a la opacidad, la falta de transparencia y, por tanto, la imposibilidad de formarse una opinión sobre las mismas.

En relación con las obligaciones de publicidad activa, la única referencia que hace la LTAIBG respecto de su incumplimiento es que el incumplimiento reiterado de las obligaciones de publicación activa tendrán la consideración de infracción grave a efectos de aplicación del régimen disciplinario establecido en las correspondientes normas.[91] En los últimos años, especialmente a partir de 2021, se han abierto expedientes sancionadores por no publicar información, tras reiterados requerimientos de los Consejos de Transparencia, pero a Ayuntamientos, como el caso del Ayuntamiento de Arcos, en Cadiz.[92]

La aprobación de la LTAIBG en 2013 supuso un importante avance a la hora de hacer más transparentes a nuestros poderes públicos y a otros sujetos obligados por la misma como los partidos políticos. Pero, casi diez años después de su aprobación, en 2022, la falta de un desarrollo reglamentario de la misma -paralizado tras el Dictamen del Consejo de Estado en 2019-,[93] parece aventurar que no habrá tal

[91] Art. 9 LTAIBG.

[92] Destacamos aquí el caso de la Ley de transparencia de la Comunidad Valenciana, donde se indica que la resolución que emita el Consejo Valenciano de Transparencia "tiene que incluir una advertencia y tiene que determinar las medidas que se tengan que adoptar para enmendar el incumplimiento y el plazo para llevarlas a cabo, que tiene que ser adecuado a la naturaleza de las medidas y que en ningún caso puede ser inferior a veinte días". Esto es, se da un plazo muy concreto para corregir las infracciones cometidas. Y ante la desatención de los requerimientos del Consejo, se indica que se podrá exigir responsabilidad e instar la incoación del procedimiento sancionador correspondiente. Y, en este sentido, se considera una infracción muy grave haber desatendido el requerimiento expreso del Consejo de Transparencia Valenciano (con un solo requerimiento sería suficiente) y se prevén multas que van de 30.001 a 100.000 euros. Vid. Arts. 13, 69 y 72 Ley 1/2022, de Transparencia y Buen Gobierno de la Comunitat Valenciana.

[93] Dictamen del Consejo de Estado de 27 de junio de 2019 sobre el Proyecto de Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (REF. 344/2019).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

desarrollo reglamentario y la reforma integral de la misma con el fin de corregir los fallos y deficiencias que se han ido evidenciando a lo largo de estos casi diez años de aplicación (Sierra Rodríguez, 2022: 37-56).

No nos detendremos en el análisis del derecho de acceso a la información pública, al que se encuentran obligadas las Autoridades de control, aunque éste forme parte de sus obligaciones de transparencia porque no guarda ninguna especificidad respecto del resto de sujetos obligados ni contribuirá al sentido de creación de las mismas en el sector de la protección de datos. Pero sí que mencionaremos los criterios a seguir cuando se ejerza el derecho de acceso y se estén tratando datos personales, derecho que las Autoridades de control están llamadas a proteger.

Así las cosas, para comprobar el grado de cumplimiento por parte de las Autoridades de control, el siguiente paso es dirigirnos a sus webs y comprobar si ofrecen la información exigida y la forma en la que lo hacen. En este sentido, la web de la AEPD recoge todas aquellas previsiones contenidas en la normativa sobre transparencia. Si bien es cierto que, en ocasiones, es difícil encontrar su contenido por la disposición o diseño de la web, lo cierto es que la información exigida se encuentra disponible. Por su parte, las webs de las Agencias autonómicas, incluida la del Consejo de Transparencia y Protección de Datos de Andalucía, recogen igualmente la información denominada publicidad activa, si bien algunas lo incluyen en apartados específicos de "transparencia" como la agencia catalana o la autoridad andaluza, y otras incluyen la información dentro del organigrama explicativo de la autoridad, como la agencia vasca. No obstante, hoy en día, no hay Administración pública, o en este caso Autoridad de control, que no tenga página web, y hacen uso de otras redes sociales de comunicación como Instagram o Twitter.

3.2.- En la normativa de protección de datos

El RGPD, que empezó a aplicarse en mayo de 2018 tras un complejo proceso de negociaciones para su puesta en marcha, se aprobó con el fin de armonizar la normativa nacional existente a nivel europeo y empoderar a los ciudadanos, favoreciendo y reforzando el mercado digital europeo (Rallo Lombarte, 2012: 15-56). La forma de conseguir estos objetivos no fue solo reducir trámites burocráticos o cargas administrativas para los responsables a la hora de tratar datos personales y otorgar más facultades a los titulares de los datos, sino plantear un nuevo enfoque proactivo frente al tradicional enfoque reactivo de la normativa (Troncoso Reigada, 2016: 464 y 468), y, para lo que aquí nos interesa, reforzando, además, la independencia de las Autoridades de control, máximes garantes del derecho fundamental a la protección de datos. El RGPD, a diferencia de la escueta atención que dedicaba la derogada Directiva 95/467CE a las Autoridades de control, que les dedicaba un único artículo (el art. 28), regula la figura de las Autoridades de control

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

independientes en su Capítulo VI (arts. 51 a 59), recogiendo en su Capítulo VII (arts. 60 a 68) las medidas de cooperación y coherencia.

Sin perjuicio de dejar aquí indicado que la transparencia es uno de los principios esenciales a la hora de tratar datos personales y sin el cual no se podrá producir el citado tratamiento,[94] el RGPD se refiere a la exigencia de transparencia en relación con las Autoridades de control sólo en una ocasión, como ahora veremos, y es en relación con el nombramiento de sus miembros, con el fin de que los mismos sean nombrados "por un procedimiento transparente", al margen de que éste se lleve a cabo en el Parlamento, por el Gobierno, por el Jefe del Estado o por un organismo independiente.[95]

Asimismo, aunque no en relación directa con las Autoridades de control, el RGPD promueve la transparencia en relación con los tratamientos de datos personales mediante la elaboración de los llamados códigos de conducta,[96] aunque sí que atribuye a las Autoridades de control el vigilar y supervisar que el código de conducta aprobado establece "procedimientos y estructuras transparentes para los interesados y el público".[97] Lo mismo que sucederá respecto de mecanismos de certificación, que estarán disponibles a través de procedimientos transparentes.[98]

En este mismo sentido, el RGPD se refiere a la transparencia, aunque no en relación con las Autoridades de control y su organización o funciones expresamente, cuando en el art. 86 regula al acceso a los documentos oficiales en poder de una Administración pública (Martínez López-Sáez, 2023: 247-256).[99] El criterio a seguir será el criterio general previsto por la LTAIBG cuando se accede a información pública que contiene datos personales. Así pues, en conexión con este derecho, debemos hacer mención aquí al conflicto existente entre transparencia y protección de datos personales cuando se solicita el derecho de acceso a la información pública y entre dicha información pública se contienen datos personales en tanto

[94] El principio de transparencia se reconoce en el art. 5.1.a) RGPD, a la vez que, en relación con el capítulo dedicado a los derechos de los interesados, el RGPD regula la "transparencia y modalidades", haciendo referencia a la transparencia de la información en su art. 12; y en el ámbito laboral se reconoce en el art. 88.2 RGPD que los Estados podrán aprobar normas adicionales al RGPD para este sector siempre prestando especial atención a la transparencia del tratamiento.

[95] Considerando 121 RGPD; y art. 53.1 RGPD.

[96] Art. 40 RGPD.

[97] Art. 41.2.c) RGPD.

[98] Arts. 42.3 y 43.2.d) RGPD y Considerando 100 RGPD.

[99] Esta previsión se contiene, sin ningún cambio en nuestra LOPDGDD en su Disp. Adic. 2ª y Disp. Final 11ª.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

que este derecho es el que deben garantizar las Autoridades de control. Con el fin de dar unas pautas para resolver dichos conflictos la LTAIBG a la hora de regular los límites del derecho de acceso en su art. 14, se remite a su art. 15 (Martínez López-Sáez, 2023: 244-247), donde se recoge el criterio general de dar el acceso cuando los datos se refieren a datos personales exclusivamente de contacto, siendo necesario el consentimiento cuando se trate de datos especialmente protegidos y requiriéndose la adecuada ponderación en el resto de supuestos. Por su parte, la LOPDGDD señala que respecto de las obligaciones de publicidad activa y acceso a la información pública cuando entre la información consten datos personales deberá encontrarse el equilibrio correspondiente, ponderándose adecuadamente.[100] La ponderación debería regir no solo para el derecho de acceso, sino también en el ámbito de la publicidad activa (Clemente Martínez, 2023: 360).

Aquí fue importante la cooperación entre la AEPD y el CTBG. Si bien es cierto que el Estatuto de la AEPD dispone la colaboración obligatoria "en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma",[101] el buen trabajo desarrollado por ambas entidades ha mejorado el nivel de transparencia en la toma de decisiones en los casos citados.

Vinculado también a la legislación de transparencia, la LOPDGDD modificó la LTAIBG para incluir la necesidad de publicar el llamado Registro de Actividades de Tratamiento[102] y para incluir un dato más a tener en cuenta a la hora de ponderar cuando se solicita el derecho de acceso en los casos en los que el afectado hubiera hecho manifiestamente públicos los datos antes de que se solicitase el acceso.[103]

Más allá de estos casos, respecto de la exigencia de una obligación de transparencia a la Autoridad de control, la LOPDGDD nos recuerda ya en su Exposición de Motivos que el RGPD refuerza el principio de transparencia.[104] Y, de la misma forma que hace

[100] Disp. Adic. Segunda LOPDGDD, con referencia a los arts. 5.3 y 15 LTAIBG.

[101] Art. 5.5 EAEPD. Vid., también Criterio Interpretativo 2/2015, del CTBG y de la AEPD, sobre Aplicación de los límites del derecho de acceso, de 24 de junio de 2015.

[102] Art. 31 LOPDGDD.

[103] Vid. Disp. Final Undécima LOPDGDD, que modifica añade un nuevo art. 6.bis a la LTAIBG y modifica el art. 15.1 LTAIBG.

[104] Apdo. III Exposición Motivos LOPDGDD: "El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

el RGPD, la LOPDGDD regula la transparencia como uno de los principios esenciales a cumplir para poder tratar datos personales, vinculándolo también a los derechos de los interesados o titulares de los datos.[105] En relación con las Autoridades de control, como ha quedado dicho, la única referencia a la transparencia la encontramos al exigir que entre las personas designadas para formar parte del Consejo Consultivo de la AEPD, una de ellas fuera "Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno".[106]

Por su parte, el EAEPD, aprobado por RD 389/2021, se adecúa a los principios propios del funcionamiento de la Administración pública, como administración independiente que son las Autoridades de control,[107] señalándose además que el citado Estatuto "asimismo, contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Agencia, al adecuarla a las nuevas competencias establecidas en dichas normas. Cumple también con el principio de transparencia, y es también adecuada al principio de eficiencia, ya que, entre otras cuestiones, no impone cargas administrativas adicionales".[108]

3.3.- Respecto de su organización, composición y funcionamiento

Entrando a analizar el grado de cumplimiento de las obligaciones de transparencia de las Autoridades de control, una vez que conocemos los requisitos normativos para su organización, composición y funcionamiento, podemos ver que es aquí donde se hace más evidente cumplir con el requisito de la transparencia, especialmente en lo que a su composición y al nombramiento de sus miembros se refiere.

---

[105] Así, vid. el Cap. I dentro del Tít. III sobre los Derechos de las personas, que regula la "Transparencia e información", recogiendo en su art. 11 la "Transparencia e información al afectado". Asimismo, la LOPDGDD reconoce como una infracción leve "el incumplimiento del principio de transparencia de la información o el derecho de información del afectado" (art. 74.a) LOPDGDD). Por otro lado, en relación con los derechos digitales el art. 80 LOPDGDD sobre el derecho a la neutralidad de Internet señala que "Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos".

[106] Art. 49.1.n) RGPD.

[107] Exposición de Motivos EAEPD que indica: "Este real decreto se adecua a los principios de buena regulación (necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia) conforme a los cuales deben actuar las Administraciones Públicas en el ejercicio de la iniciativa legislativa y la potestad reglamentaria, según establece el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas".

[108] Exposición de Motivos EAEPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Ya hemos visto que, al contrario de lo que exige el RGPD respecto del procedimiento transparente para la elección de los miembros de las Autoridades de control, la LOPDGDD no dice nada al respecto. Y si bien es cierto que la LOPDGDD y el EAEPD han previsto un procedimiento dotado de más garantías para asegurar la independencia de la Autoridad, la falta de transparencia en alguno de sus extremos provocó que en el primer nombramiento de la AEPD bajo el nuevo sistema fuera objeto no sólo de críticas por doctrina y medios de comunicación, sino que acabará en los Tribunales (García Mahamut, 2023).[109] Aunque la Orden por la que publicó la convocatoria del proceso selectivo se hizo en noviembre de 2021, en octubre ya se había publicado a través de los medios de comunicación los nombres de las personas que iban a ocupar tanto la Presidencia como el cargo de Adjunto a la AEPD, sin esperar a cumplir con los principios de mérito y capacidad constitucionalmente exigidos para el acceso a la función pública, como muy bien se ha señalado (García Mahamut, 2023: 179 y 181).[110]

En realidad, la LOPDGDD ha optado por una fórmula un tanto confusa para el nombramiento y designación tanto de la Presidencia como del Adjunto/a, tanto en términos de transparencia como de independencia.[111] No obstante, es cierto que el nombramiento de la Presidencia, y también ahora de un Adjunto o Adjunta, no cae solo en manos del Gobierno, sino que se deberá haber oído previamente al Congreso sobre la justificación del candidato propuesto respecto de su mérito, capacidad, competencia e idoneidad, y cuya elección el Congreso debe ratificar en la Comisión de Justicia por una mayoría cualificada en primera votación de 3/5, y de una mayoría absoluta en segunda (Arenas Ramiro, 2019a).

Como se ha señalado, el proceso de selección de la primera Presidencia y Adjuntía conforme a la nueva LOPDGDD, parecía seguir este procedimiento, a pesar de las noticias que saltaron a la prensa, y tras la correspondiente presentación de candidaturas, se emitió una Orden publicando el Acuerdo del Consejo de Ministros con el nombre de las mismas personas que se habían publicitado en los medios de comunicación, aunque eso sí, entre una terna que se remitió al Congreso de los

[109] Vid. STS 608/2022, de 24 de mayo de 2022.

[110] Vid. Orden JUS/1260/2021, de 17 de noviembre, por la que se convoca proceso selectivo para la designación de la Presidencia y de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.

[111] Así lo ha indicado el Dictamen del Consejo de Estado, de 11 de febrero de 2021 (nº 683/2020).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Diputados.[112] La citada Orden fue impugnada por uno de los candidatos y el Tribunal Supremo entre sus pronunciamientos señaló que "en coherencia con la condición de la AEPD como administración independiente, la vigente normativa regula un procedimiento de selección concurrencial, público y transparente, donde un comité selecciona a los candidatos, hace una propuesta al Consejo de Ministros, que debe remitir el nombre de un candidato para cada uno de los dos cargos al Congreso para su ratificación, pero no una terna por orden alfabético". Y así, tras suspender el proceso, el Tribunal Supremo vino a destacar "el daño en término reputacional para la AEPD, dentro de España y ante la Unión Europea" ante este tipo de hechos (para seguir el procedimiento, con un excelente análisis crítico y propuestas de mejora, vid. García Mahamut, 2023).

Al margen del escándalo que esto provocó, no sólo en términos jurídicos, resulta un tanto curioso que se utilicen los términos de idoneidad, o se hable de personas de reconocida competencia profesional, no sólo por la indeterminación del concepto de lo idóneo, sino porque se señala expresamente que dicha competencia lo sería "en particular, en materia de protección de datos", permitiéndose, por lo tanto, que la competencia pudiera ser en otras materias, no exigiéndose tampoco, como se hace en otros países de nuestro entorno, un número mínimo de años de experiencia acreditada.

En conexión con la valoración de los candidatos a los puestos de Presidencia y Adjuntía, teniendo en cuenta los criterios antes mencionados y que deberá valorar un Comité de selección,[113] se ha criticado que a falta de una concreción sobre los criterios para valorar el mérito, la capacidad, la competencia y la idoneidad o requisitos de "titulación, experiencia y aptitudes", se debería "al menos, articular un procedimiento transparente para la designación del candidato que será propuesto por el Ministerio de Justicia, en aras de garantizar su independencia" (García Mahamut, 2023: 194).[114]

Asimismo, si tenemos en cuenta el actual juego político y las mayorías parlamentarias existentes, quizá hubiera sido preferible, como sucede con el Defensor del Pueblo, la intervención de las dos Cámaras o de una Comisión mixta de ambas en su nombramiento. No podemos olvidar que la AEPD, como el Defensor del Pueblo son garantías institucionales al servicio y protección de derechos

[112] Vid. Orden JUS/133/2022, de 26 de febrero, por la que se publica el Acuerdo del Consejo de Ministros de 22 de febrero de 2022, por el que se comunica al Congreso de los Diputados la propuesta de candidatos a ocupar la Presidencia y la Adjuntía de la Agencia Española de Protección de Datos.

[113] Art. 20 EAEPD.

[114] Vid. Dictamen 683/2020, del Consejo de Estado, de 2 de junio de 2021.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

fundamentales. No obstante, a pesar de que parece mucho más independiente el hecho de que el nombramiento venga por un organismo independiente o por una mayoría cualificada del Parlamento, en España hemos seguido vinculando el nombramiento a una decisión del Ministro de Justicia, esto es, del Gobierno. La falta de transparencia en el proceso que vuelve a caer en las mismas manos resta nuevamente independencia al órgano con el peligro que esto comporta para la defensa de nuestros derechos fundamentales.

En relación con su personal, y concretamente con su estatuto personal, se establece un régimen de incompatibilidades, junto con toda una serie de derechos y obligaciones. Pero es en este punto donde el RGPD, de nuevo, vuelve a dejar en manos de los Estados miembros, su configuración.[115] El RGPD se limita a señalar que los miembros de las Autoridades de control deben actuar con "integridad" con el fin de garantizar la independencia de la institución.[116] Por ello, los miembros de las Autoridades de control no podrán llevar a cabo "cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no".[117] En este sentido, aunque la LOPDGDD se remite a las normas del Sector público, será el EAEPD el que configure dichos extremos. Aquí, sería realmente interesante que, como apunta el RGPD,[118] los Estados, en este caso España, recogieran en dicho Estatuto no sólo la acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato, sino que se regularan también dichas incompatibilidades después del mismo, con el fin de no abrir las conocidas "puertas giratorias" en este tipo de puestos y que lógicamente, empañan su independencia (Troncoso Reigada, 2016: 479-480).

También en relación con su personal, con lo que tiene que ver con los recursos humanos de estas Autoridades de control, el CEPD advirtió en 2021 del hecho de que casi un 90% de las Autoridades de control (incluyendo las españolas), no disponían de recursos suficientes para llevar a cabo sus funciones. Si ponemos este hecho en conexión con el aumento de multas impuestas en los últimos años, la sombra de la sospecha sobre la falta de independencia y de transparencia en su imposición, asoman rápidamente (Viguri Cordero, 2022: 261).[119] Asimismo, esta falta

115 Art. 52.3 RGPD.

116 Considerando 121 RGPD.

117 Art. 52.3 RGPD.

118 Art. 54.1.f) RGPD.

119 Vid. CEPD, Descripción general de los recursos puestos a disposición de las Autoridades de protección de datos por los Estados miembros y de las acciones de ejecución por parte de las Autoridades de protección de datos, de 5 de agosto de 2021.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

de recursos humanos afecta también a la capacidad de la Autoridad de control para hacer frente a sus obligaciones de publicidad activa. La falta de personal que se pueda ocupar de publicar información implica no cumplir o cumplir inadecuadamente con las obligaciones de transparencia activa (Clemente Martínez, 2023: 361-362).

Por último, el RGPD aborda también las obligaciones del personal que trabaja en la autoridad de control e insiste en el deber de secreto profesional, no sólo durante el mandato, sino incluso finalizada el mismo,[120] haciéndose especial hincapié a la información relacionada con las infracciones cometidas en este terreno.[121]

Así las cosas, sobre el régimen del personal de las Autoridades de control, no parece tener mucho sentido que su selección, obligaciones, derechos o garantías difieran de lo dispuesto para los funcionarios y empleados que trabajan en cualquier Administración pública (Troncoso Reigada, 2016: 481), pues las Autoridades de control, más aún si cabe que cualquier otra Administración pública por la especial función que cumplen, deben servir con objetividad a los intereses generales, como se deriva del mandato constitucional contenido en el art. 103 CE, destacándose así la necesidad de transparencia en estos procesos.

Por lo que respecta al funcionamiento de las Autoridades de control y a la necesidad de las mismas de contar no sólo con recursos humanos, sino también económicos para hacer frente a sus funciones, encontramos algún que otro problema. Un problema lo vamos a encontrar en el hecho de la falta de recursos económicos destinados a adquirir herramientas informáticas o aplicaciones que faciliten cumplir con las obligaciones de transparencia activa y dar respuesta en el ejercicio del derecho de acceso y mantener actualizados sus portales de transparencia. Si no cuentan con los recursos materiales suficientes, no se podrá hacer frente de forma adecuada a sus obligaciones y no tendremos Administraciones eficientes (Clemente Martínez, 2023: 363-365).

Para concluir, podríamos decir en relación con la organización, composición y funcionamiento de las Autoridades de control, que su nivel de transparencia dependerá no sólo de las personas que las dirigen, sino de la voluntad política de quien tiene que destinar los recursos para las mismas (Clemente Martínez, 2023: 367-370).

---

[120] Art. 54.1.f) RGPD. Sobre este deber de secreto, véase también la STJUE de 16 de octubre de 2012, Comisión europea contra Austria (C-614-/10), §§ 62-64, con referencia a la posibilidad de que ante la ausencia de un deber de secreto se pudiera someter a la Autoridad de control a una influencia indirecta incompatible con las exigencias de independencia de la normativa.

[121] Art. 54.2 RGPD.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Pero, a pesar de todo lo dicho, y de la conexión existente entre falta de transparencia y ausencia de independencia, si nos limitamos a fijarnos en las webs de las Autoridades de control, podremos comprobar, como ya hemos dicho, cómo cumplen con sus obligaciones respecto de la publicidad activa. Así, por ejemplo, veremos que la APDCAT y el CTPD andaluz tienen una pestaña específica y visible destinada a "Transparencia", y la AEPD y la AVPD también, aunque dentro de la pestaña dedicada a la "Agencia". Todas las Autoridades de control tienen en sus páginas web información relativa a las obligaciones de publicidad activa que marca la LTAIBG. Así, todas tienen información institucional, organizativa (incluyen incluso todas ellas, excepto la APDCAT, el cv de sus órganos de dirección), de relevancia jurídica, sobre contratos, convenios y subvenciones, así como información económica, financiera y presupuestaria.

Analizando pues el grado de cumplimiento en materia de publicidad activa, el CTBG se ha pronunciado sobre el grado de cumplimiento de la AEPD, pero su resultado sería fácilmente trasladable al resto de Autoridades autonómicas. El CTBG ha señalado en su Informe de revisión de 2022 de la AEPD que "No puede menos que valorar muy positivamente la evolución del cumplimiento de las obligaciones de publicidad activa por parte de la AEPD. (…) Bastaría con que se publicase información sobre las modificaciones de contratos y el organigrama en formato reutilizable para que el nivel de cumplimiento se sitúe en el 100%", dado que a febrero de 2022 se encontraba en un 95,2%.

En conclusión podemos comprobar que las Autoridades de protección de datos son activamente transparentes en lo que a su organización, composición y funcionamiento se refiere, pero si tenemos en cuenta los problemas que se han detallado respecto del nombramiento de sus órganos de dirección, podemos comprobar cómo la transparencia se cumple formalmente e, incluso, sirve para ocultar técnicas consolidadas en la práctica y que obedecen a una falta de cultura pública y de respeto no sólo por la separación de poderes, sino de respecto por las instituciones que deben estar diseñadas para defender los derechos fundamentales de los ciudadanos.

3.4.- Respecto de sus competencias y funciones

En relación con las funciones y la necesidad de transparencia en su ejercicio, debemos señalar que sólo de forma transparente se podrá comprobar que las funciones no son ejercidas fruto de mandato alguno. Como exige el RGPD, las funciones de las Autoridades de control deberán ser llevadas a cabo con total independencia. El RGPD dispone que las Autoridades de control no estarán sometidas a orden o instrucción alguna, de la misma forma que lo venía exigiendo la Directiva 95/46/CE y de la misma forma que lo venía exigiendo el TJUE en sus Sentencias, pero concreta que los miembros de dichas Autoridades serán "ajenos a

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción"[122]. Esto sólo se puede comprobar si las decisiones tomadas están debidamente publicadas y es accesible la forma y los criterios conforme a los cuales se ha tomado la decisión.

Así las cosas, debemos destacar que el RGPD hace especial hincapié en la actitud proactiva que deben llevar a cabo las Autoridades de control, lo que se detallará por cada uno de los Estados. Esta proactividad refuerza el resto de funciones y se va a manifestar, entre otras, y especialmente, en funciones orientadas a la sensibilización y concienciación y a ofrecer una información comprensible, lo que redundará en último término en una mayor transparencia del sector. En esta línea, dentro de las funciones que corresponden a la Subdirección General de Promoción y Autorizaciones de la AEPD, el EAEPD le atribuye "El ejercicio de las funciones que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, atribuye a las Unidades de Información"[123].

Así, por ejemplo, con el fin de dar publicidad a sus actuaciones, la LOPDGDD exige la publicación en la página web de la AEPD de las resoluciones de la Presidencia relacionadas, por ejemplo, con la atención a las facultades del derecho a la protección de datos o con aquéllas que impongan medidas cautelares, así como "toda aquella información que la Presidencia considere relevante y que contribuya al mejor cumplimiento de sus funciones".[124] De la misma forma, nuestra LOPDGDD reconoce expresamente como "otras potestades de la Agencia Española de Protección de Datos",[125] la potestad de regulación mediante la elaboración y aprobación de Circulares que tendrán carácter vinculante una vez publicadas en el BOE (Arenas Ramiro, 2019a: 265-267). El EAEPD desarrolla el procedimiento de elaboración de estas Circulares, estableciendo un trámite de audiencia pública mediante la publicación en la web de la AEPD por un tiempo que variará de quince a siete días "por razones debidamente motivas que así lo justifiquen" y sólo podrá omitirse "cuando existan graves razones de interés público, que deberán justificarse

[122] Art. 52.2 RGPD.

[123] Art. 28.p) EAEPD.

[124] Art. 11 EAEPD. Así, el 20 de abril de 2023 la AEPD ha publicado por primera vez un Listado con las Administraciones públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas. Vid. https://www.aepd.es/es/areas-de-actuacion/administraciones-publicas/administraciones-publicas-sancionadas.

[125] Sección 3ª del Capítulo I, del Título VII, LOPDGDD (arts. 55 y 56).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

en el informe técnico".[126] Destacamos la importancia de las Circulares en tanto que serán las mismas las que se deberán aprobar en relación con las medidas de seguridad a implementar, por lo que cobrarán un gran valor entre responsables del tratamiento de datos, en tanto que es un ámbito que el RGPD ha dejado abierto al buen saber y entender de cada responsable y a su voluntad proactiva[127].

Por último, una de las competencias en las que será necesaria un mayor grado de transparencia lo vamos a encontrar en relación con las competencias sancionadoras y de investigación y con las funciones de coherencia, especialmente porque es en relación con estos poderes de investigación cuando se plantean los problemas relacionados con la división de competencias entre las distintas Autoridades de control.[128] El RGPD incluye disposiciones que tratan de dar solución a estos problemas mediante los conocidos como mecanismos de ventanilla única y las obligaciones de cooperación entre las Autoridades de control, y lo mismo reproduce la LOPDGDD. Es aquí donde se hace imprescindible cumplir con los requisitos de transparencia por parte de cada una de las Autoridades de control que intervengan en el correspondiente procedimiento. La falta de transparencia implicará que una Autoridad no pueda acceder a la información o tenga un conocimiento completo de los hechos producidos y de las actuaciones llevadas a cabo con la repercusión en el derecho a la protección de datos respecto del titular afectado.

Revisando las páginas webs de las Autoridades de control en protección de datos, se puede comprobar cómo las Autoridades sí que recogen y detallan los procedimientos que siguen y cuáles son sus competencias.

Por ello, tenemos que concluir que el problema jurídico no se va a producir en relación con la publicación de las competencias y funciones que las mismas desarrollan. Como hemos visto, las Autoridades publican incluso documentación orientada a ayudar a los ciudadanos en los procedimientos ante las mismas, por ejemplo, como sucede con el CTPD andaluz mediante la publicación de información sobre procedimientos y cartas de servicios, a pesar de que éste no la tenga

[126] Art. 55 LOPDGDD; y art. 6 EAEPD. En marzo de 2019 se aprobó la primera Circular de la AEPD: 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 (BOE de 11 de marzo de 2019).

[127] Nos remitimos aquí a las Circulares ya citadas, destacando la Circular 1/2023, conocida como la Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas. Contribuye así la AEPD a clarificar el ejercicio del derecho en este terreno.

[128] Sobre este tema se pronunció el TJUE en la Sentencia de 1 de octubre de 2015, Weltimmo contra Nemzeti Adatvédelmi és Információszabadsag Hatósag (C-230/14).

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

actualmente, como sucede también con la APDCAT; o disponen de un Canal ético con códigos éticos y con canales de denuncia internos, como sucede también con el CTPD andaluz, o de Quejas y sugerencias como en la AEPD, en la APDCAT y en la AVPD; o, incluso, tienen un apartado de Evaluación de los servicios como en la APDCAT (aunque un poco desactualizado, con información sobre unas Jornadas llevadas a cabo a lo largo de 2019) o el excelente seguimiento llevado a cabo por el CTPD andaluz.

Así pues, el problema no vendrá por la publicidad de la actividad, de las funciones que llevan a cabo, que viene mayormente recogida, sino en los criterios para llevarlas a cabo, como hemos visto que sucedía en relación con los procedimientos sancionadores y los criterios de imposición de multas. Siendo estas cuestiones las que, debido a la falta de transparencia, crean más inseguridad jurídica y más desconfianza ciudadana. La publicación de criterios claros y definidos en cuanto a las competencias atribuidas a estas Autoridades reforzaría su independencia y, por tanto, su razón de ser.

4.- A modo de reflexión

A lo largo del presente artículo hemos podido analizar el por qué de la existencia de Autoridades administrativas independientes a la hora de garantizar, para el caso que aquí nos interesa, el derecho fundamental a la protección de datos personales, la necesidad de su creación en este sector.

Constatada su necesidad, analizada su organización y funciones o competencias, hemos comprobado cómo las mismas se ven sometidas a las obligaciones de transparencia y cómo, aparentemente, las Autoridades de protección de datos españolas, formalmente, cumplen con estas obligaciones, como lo demuestran sus páginas webs. Pero la cuestión va más allá de su cumplimiento estético, como hemos podido analizar y como hemos visto reflejado en el proceso de nombramiento de los puestos de Presidencia y Adjuntía de la AEPD.

La ausencia de una transparencia, que podríamos calificar "de fondo", provoca que el verdadero motivo que justificaba la creación de este tipo de Autoridades pierda todo su sentido. Se requieren no sólo garantías formales, sino sustanciales que permitan afirmar que estamos verdaderamente ante una Administración pública independiente, lejos de cualquier sesgo político y destinada, en este caso, a garantizar un derecho fundamental.

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Bibliografía

ARENAS RAMIRO, M. 2019a. "Artículo 55", en Arenas Ramiro, M. / Ortega Giménez, A, *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Madrid: SEPIN, pp. 265-267.

ARENAS RAMIRO, M. 2019b. "Artículo 47", en Arenas Ramiro, M. / Ortega Giménez, A, *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Madrid: SEPIN, pp. 229-234.

ARENAS RAMIRO, M. 2019c. "Artículo 48", en Arenas Ramiro, M. / Ortega Giménez, A, *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Madrid: SEPIN, pp. 235-240.

ARENAS RAMIRO, M. 2021. "RGPD y Autoridades de protección de datos: Un antes y un después" en Tomás Mallén B., Garcia Mahamut, R. y Pauner Chulvi (Eds.), *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español. Cuestiones clave de orden nacional y europeo*. Valencia: Tirant lo Blanch.

ARENAS RAMIRO, M. 2022. "Data protection in Latin America", en González Fuster, G. / Van Brakel, R. / De Hert, P. (Eds.), *Research Handbook on privacy and data protection law*. Reino Unido: Edwar Elgar Publishing, pp. 139-160.

BETANCOR RODRÍGUEZ, A. 1994. *Las Administraciones independientes: un reto para el Estado social y democrático de derecho*. Madrid: Tecnos.

BLANCO ANTÓN, M.J. 2018. "Capítulo XXX. Autoridades de control independientes (arts. 51-59)", en López Calvo, J. (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Madrid: Bosch / Wolters Kluwer, pp. 591-607.

BLANES CLIMENT, M.A. 2014. "Sin transparencia no hay democracia", en *Cuadernos Manuel Giménez Abad*, núm. 8, pp. 151-158.

CERVERA NAVAS, L. 2016. "El Comité Europeo de Protección de Datos", en Piñas Mañas, J.L. (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, pp. 527-538.

CLEMENTE MARTÍNEZ, J. 2023. "La protección de datos personales en la gestión de la transparencia activa por parte de las Entidades locales", en Tomás Mallén, B. / García Mahamut, R., *La implementación del Reglamento General de Protección de*

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

Datos en España y el impacto de sus cláusulas abiertas. Valencia: Tirant lo Blanch, pp. 359-385.

DELGADO MORALES, F. 2017. "Percepción ciudadana de la transparencia", en SÁNCHEZ DE DIEGO, M. (Coord.), *Visiones actuales de la transparencia*. Madrid: DMK Consultores, pp. 310-324.

GARCÍA MAHAMUT, R. 2019. "Del Reglamento General de Protección de Datos a la LO 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales", en García Mahamut, R. / Tomás Mallén, B., *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado*. Valencia: Tirant lo Blanch, pp. 95-131.

GARCÍA MAHAMUT, R. 2023. "Graves anomalías en el primer proceso de selección de la Presidencia y Adjuntía de la AEPD al amparo de la LOPDGDD y del RGPD: algunas propuestas de reforma", en Tomás Mallén, B. / García Mahamut, R., *La implementación del Reglamento General de Protección de Datos en España y el impacto de sus cláusulas abiertas*. Valencia: Tirant lo Blanch, pp. 177-197.

GONZÁLEZ FUSTER, G. 2019. "El Comité Europeo de Protección de Datos (CEPD): territorio desconocido", en García Mahamut, R. / Tomás Mallén, B., *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado*. Valencia: Tirant lo Blanch, pp. 161-180.

GUICHOT REINA, E. 2017. "Transparencia y acceso a la información en las entidades locales vascas", en: *RVAP*, núm. 107-II.

GUTIÉRREZ DAVID, E. 2014. "Derecho de acceso a la información pública", en *Eunomía. Revista en Cultura de la Legalidad*, núm. 6.

IRURZUN MONTORO, F. 2016. "XXVII. Cooperación y coherencia entre Autoridades de control", en Piñas Mañas, J.L. (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, pp. 513-526.

LÓPEZ CALVO, J. 2017. *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid: Sepín.

LÓPEZ CALVO, J. 2018. "Capítulo XXXI. Cooperación y coherencia", en López Calvo, J. (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Madrid: Bosch / Wolters Kluwer, pp. 609-632.

MARTÍNEZ LÓPEZ-SÁEZ, M. 2021. "La ratificación española del Convenio 108+: consideraciones jurídicas básicas del nuevo marco Paneuropeo de protección de datos", en *Revista General de Derecho Europeo*, núm. 54.

Sección Estudios y Artículos
Las obligaciones de transparencia en las Autoridades de protección de datos
por Mónica Arenas Ramiro
Págs. 227-270
DOI: https://doi.org/10.51915/ret.312

MARTÍNEZ LÓPEZ-SÁEZ, M. 2023. "El impacto de las cláusulas abiertas del RGPD en materia de transparencia y acceso a la información pública", en TOMÁS MALLEN, B. / GARCÍA MAHAMUT, R., *La implementación del Reglamento General de Protección de Datos en España y el impacto de sus cláusulas abiertas*. Valencia: Tirant lo Blanch, pp. 231-259.

MARTÍNEZ MARTÍNEZ, R. (Dir.), 2019. *Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales. Edición especial*, Madrid: Wolters Kluwer.

PAUNER CHULVI, C. / TOMÁS MALLÉN, B. (Coords.). 2009. *Las Administraciones independientes*. Valencia: Tiran lo Blanch.

POMED SÁNCHEZ, L.A. 1993. "Fundamento y naturaleza jurídica de las Administraciones independientes", en *Revista de Administración Pública*, núm. 132, pp. 117-169.

RALLO LOMBARTE, A. 2009. "Las Administraciones independientes: una aproximación constitucional", en PAUNER CHULVI, C. / TOMÁS MALLÉN, B. (Coords.). 2009. *Las Administraciones independientes*. Valencia: Tiran lo Blanch, pp. 11-19.

RALLO LOMBARTE, A. 2012. "Hacia un sistema europeo de protección de datos: las claves de la reforma", en *RDP*, núm. 85, pp. 15-56.

SALA ARQUER, J.M. 1984. "El Estado neutral. Contribución al estudio de las administraciones independientes", en *REDA*, nº 42.

SALVADOR MARTÍNEZ, M. 2002. *Autoridades independientes. Un análisis comparado de los Estados Unidos, el Reino Unido, Alemania, Francia y España*, Barcelona: Ariel.

SALVADOR MARTÍNEZ, M. 2019a. "Artículo 44", en Arenas Ramiro, M. / Ortega Giménez, A, *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Madrid: SEPIN, pp. 219-221.

SALVADOR MARTÍNEZ, M. 2019b. "Artículo 45", en Arenas Ramiro, M. / Ortega Giménez, A, *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Madrid: SEPIN, pp. 222-224.

SIERRA RODRÍGUEZ, J. 2022. "Enfoques ante una reforma de la Ley de Transparencia. Especial referencia a la transparencia informativa del Gobierno", en *Revista Española de Transparencia (RET)*, núm. 14, pp. 37-56.

SORIANO MORENO, S. 2019. "Artículos 57 a 59", en Arenas Ramiro, M. / Ortega Giménez, A, *Protección de datos. Comentarios a la Ley Orgánica de Protección de*

CC BY SA

Datos y Garantía de Derechos Digitales (en relación con el RGPD). Madrid: SEPIN, pp. 272-278.

TRONCOSO REIGADA, A. 2005. "Las Comunidades Autónomas y la protección de datos personales: marco constitucional y posibilidades para el futuro", en *Revista parlamentaria de la Asamblea de Madrid, núm. 12.*

TRONCOSO REIGADA, A. 2009. "Las Agencias de Protección de Datos como Administración independiente", en Pauner, C. / Tomás, B., *Las Administraciones independientes*. Valencia: Tirant lo Blanch, pp. 27-216.

TRONCOSO REIGADA, A. 2016. "XXVI. Autoridades de control independientes", en Piñas Mañas, J.L. (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, pp. 461-512.

VIGURI CORDERO, J.A. 2015. "Cooperación y coordinación entre autoridades de protección de datos", en Rallo Lombarte, A. / García Mahamut, R. (Coords.), *Hacia un nuevo derecho europeo de protección de datos*. Valencia: Tirant lo Blanch, pp. 739-769.

VIGURI CORDERO, J.A. 2021. "*La adopción de instrumentos de certificación como garantía eficiente en la protección de los datos personales", en Revista Catalana de Dret Públic,* núm. 62, pp. 160-176.

VIGURI CORDERO, J.A. 2022. *"El papel de las Autoridades europeas de protección de datos en su apuesta por* acciones preventivas y/o reactivas", en *Revista General de Derecho Europeo*, núm. 57, pp. 241-271.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023: un derecho en vías de consolidación

Jorge Viguri Cordero[1]
Universitat Jaume I (UJI)
España

ORCID: 0000-0001-6994-7057

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

El presente artículo se ha realizado en el marco del proyecto de investigación del Ministerio de Ciencia e Innovación DATATRANSCO con referencia n.º PID2021-128309NB-I00.

RESUMEN: El 20 de febrero de 2023, se aprobó la Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, por la que transpone la Directiva 2019/1937 relativa a la protección de las personas que denuncian infracciones del Derecho de la Unión. El objeto del presente estudio radica en poner de relieve el deficitario proceso de transposición de esta Directiva, especialmente, de aquellos aspectos más críticos que contempla esta ley. Consecutivamente, se acomete el margen de mejora que requieren algunos preceptos legales que no solo comprometen la efectividad de este acto legislativo de la Unión Europea, sino que generan dudas de encaje constitucional con otras normas nacionales de carácter general y sectorial. Finalmente, se identifican algunas de las lagunas más destacadas que presenta el ámbito objetivo y subjetivo de la ley española con un fiel reflejo de otras

[1] Profesor Permanente Laboral de Derecho Constitucional y Secretario de la Facultad de Ciencias Jurídicas y Económicas. Universitat Jaume I. Su ámbito de investigación se ha centrado en el ámbito del derecho a la protección de datos de carácter personal y el derecho a la protección internacional. Cuenta con 1 sexenio de investigación concedido por la CNEAI. Es autor de 1 monografía editada por Tirant lo Blanch, 2020 (pp. 1-415), ha coordinado 2 obras colectivas y cuenta con una veintena de artículos y de capítulos de libro publicados en revistas y editoriales de impacto.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

legislaciones europeas más consolidadas, para así proponer a modo de *lege ferenda* respuestas sobre las que debería pivotarse una futura reforma de la misma.

PALABRAS CLAVE: informante, corrupción, especificación nacional, infracciones.

CONTENIDOS: 1.-Introducción. 2.-Retos más inmediatos que plantea la aplicación de la Ley 2/2023 de protección al informante. *2.1.-Aspectos clave de la transposición española. 2.2.- Cuestiones más problemáticas de la Ley 2/2023 de protección de las personas informantes.* 3.-La aplicación material y personal de la Ley 2/2023: algunos aspectos críticos. 3.1.-El ámbito de aplicación material u objetivo. 3.2.-El ámbito de aplicación personal o subjetivo. 4.-Reflexiones conclusivas. -Bibliografía.

Challenges in the protection of whistleblowers in Spain after the approval of the Law 2/2023: a consolidating right

ABSTRACT: On February 20, 2023, Law 2/2023 on the regulation of the protection of individuals reporting regulatory infringements and combating corruption was approved, thereby transposing Directive 2019/1937 on the protection of persons reporting breaches of Union law. The purpose of this study is to highlight the inappropriate transposition process of this Directive, especially most critical aspects covered by this law. Consecutively, the margin for improvement required by some of its precepts is undertaken, which not only compromises the effectiveness of the legal act of the European Union, but also raises doubts concerning ownership of national and sectoral legislation. Finally, some gaps with regard to the objective and subjective scope of this Spanish law are identified, with a faithful reflection of those national legislations that are more consolidated with the aim to propose some answers as a *lege ferenda* on the future reform of the law.

KEYWORDS: whistleblower, corruption, national specification, breaches.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

1.- Introducción

Las personas informantes poseen un papel fundamental en los países democráticos, son los que alertan sobre irregularidades y prácticas que son inaceptables para las sociedades democráticas y perjudiciales para el interés general. Una legislación consolidada en esta materia fomenta la integridad, la cual es considerada una de las piedras angulares de las estructuras políticas, económicas y sociales que contribuye al desarrollo y bienestar económico y social.[2] Indudablemente, la transparencia a la que pueden contribuir los denunciantes resulta esencial para que las instituciones sean eficaces y rindan cuentas en todos los niveles, ayudando a erradicar –o, cuanto menos reducir– los casos de corrupción o de actividades ilegales o poco éticas.

Por lo que concierne a España, uno de los principales obstáculos para la implementación de un modelo integral de *whistleblowing* ha partido de la falta de sustrato para poder insertar con cierto éxito un instrumento que ha permanecido ajeno a nuestra cultura jurídica. Los casos de corrupción en nuestro país, yuxtapuesto a factores de diversa índole de naturaleza sociocultural relacionados con el carácter peyorativo que gira en torno a la figura del informante, el temor a potenciales represalias, en sintonía con una mala reputación social que se ha derivado de tal acción[3] socavó gravemente la implementación de un marco jurídico eficaz y efectivo de protección a las personas informantes en las pasadas décadas.

De hecho, el tradicional término de denunciante en nuestro país –dimanante de la directa traducción directa del tradicional concepto anglosajón de *whistleblower*–[4] ha estado estrictamente relacionada con un antiguo estatuto –aún vigente– previsto por el Decreto de 14 de septiembre de 1882 sobre el procedimiento penal español por el que se imponen algunas obligaciones a las personas a la hora de denunciar. Una definición que no ha permanecido ajena a características estigmatizantes,[5] a pesar de la legislación nacional sectorial relativa a protección de datos de carácter personal o de lucha contra la corrupción que comenzó a aprobarse a en España a

[2] Esta promueve la consecución de los objetivos de desarrollo sostenible (ODS) de las Naciones Unidas, muy especialmente el núm. 16 relativo a "Paz, Justicia e Instituciones Sólidas".

[3] Sobre la compleja implementación de un modelo de *whistleblowing* en España, véase: PÉREZ MONGUIÓ (2020: 232 - 233).

[4] En torno a la figura del whistleblower en la experiencia de common law, remitimos a los siguientes estudios: BENÍTEZ PALMA (2018: 13-16); PÉREZ TRIVIÑO (2018:287); RAGUÉS I VALLÉS (2006: 3).

[5] Para un análisis de las distintas denominaciones en torno a la figura del "whistleblower" en Europa, véase: CHEVARRÍA, SILVESTRE (2013).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

partir de la década de los 80.[6] Así, la ausencia de una norma general y jurídicamente vinculante a nivel estatal susceptible de aplicación a distintos ámbitos y sectores propició que la mayor parte de potenciales denunciantes adoptaran una actitud pasiva, evitando denunciar ya sea porque la acción de informar no ha gozado de suficiente respaldo social o, simplemente, porque consideraban que no estaban protegidos frente a represalias de distinta índole.

En efecto, España no seguía la senda de algunos Estados miembros, como en es el caso de Francia, donde se han ido aprobado leyes relativas a la protección a los "lanzadores de alertas" –del término en francés, *"lanceurs d'alerte"*– que, como tendremos ocasión de abordar posteriormente, fueron consolidándose con el transcurso de los años. Sin embargo, en el plano europeo, era más que constatable una protección fragmentada, pues algunas legislaciones nacionales protegían exclusivamente a los empleados públicos, otras al sector privado mientras que otros Estados o se limitaban a prever irregularidades específicas o, sencillamente, no contemplaban protección alguna en este sentido.[7] Basta recordar a Guido Strack (2011: 115-116), exfuncionario de la UE, cuando alertó a principios de la década pasada que la legislación de protección de los denunciantes en muchas naciones había resultado tan limitada que, en numerosas ocasiones, se apreciaba una falsa apariencia de protección real.

No fue hasta el 23 de octubre de 2019 cuando se produjo un momento clave, como fue la aprobación de la Directiva 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (en adelante, Directiva de protección de los denunciantes),[8] la cual confiere protección a las personas que, conocedoras de infracciones de las organizaciones públicas o privadas para las que

[6] El término denunciante comenzó a distanciarse de términos eminentemente peyorativos cuando comenzaron a crearse algunas autoridades nacionales de protección de datos o agencias anticorrupción. Sobre el particular, remitimos a: GARCÍA MORENO (2020: 285-289) y (2022: 39-40).

[7] Comisión europea, Documento de Trabajo del personal de la Comisión: Evaluación de Impacto que acompaña al documento de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de las personas que informen sobre infracciones del Derecho de la Unión, SWD(2018) 116 final, 23 de abril de 2018, p. 3.

[8] Esta Directiva entró en vigor el 16 de diciembre del año 2019 y su art. 26 fijó un plazo de hasta dos años para su efectiva transposición, esto es, hasta el 17 de diciembre de 2021 –con excepción de las entidades jurídicas del sector privado de entre 50 y 249 trabajadores, cuyo plazo se prorrogó dos años más a fin de que los Estados miembros aprobaran en sus respectivas legislaciones nacionales aquellas especificaciones relativas a la obligación de establecer canales de denuncias internas para aquellas empresas de 50 o más trabajadores– (Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, L 305/17). Para un análisis sobre la citada Directiva, véase, entre otros: Fernández Ajenjo (2020: 111-139); Villoria Mendieta (2021: 15-24).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

trabajan o prestan servicios o tienen conexión de alguno de los tipos que establece, puedan denunciarlas sin temor a posibles represalias. Se trata de un texto sumamente innovador cuyo principal objetivo ha radicado en lograr un marco legal supranacional uniforme para la implementación de sistemas de denuncia y protección de las personas informantes o denunciantes en la totalidad de los Estados miembros mediante el establecimiento de un marco jurídico legalmente vinculante que avance en el reconocimiento del derecho fundamental a una buena administración que contempla el art. 41 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE).

Esta Directiva proporciona una base sólida mediante el establecimiento de unos estándares mínimos de protección y cuya efectividad se ha supeditado a la ulterior transposición por parte de los de Estados miembros –al margen de otra normativa específica existente en lo que afecta a algunas reglas sobre la denuncia, presentación de informes y divulgación de irregularidades–.[9] Así, cada Estado miembro ha especificado un amplio conjunto de mecanismos jurídicos y garantías y cuentan, además, con una oportunidad sin precedentes, esto es, la posibilidad de prever un tratamiento más favorable en las respectivas legislaciones nacionales para los derechos de los informantes o denunciantes. Dicho de otro modo, la especificación de la Directiva en sede nacional "en ningún caso" puede constituir motivo para reducir el nivel de protección (art. 25) y, *sensu contrario,* la operatividad de la cláusula de no regresión supone que sus disposiciones no permiten disminuirlo tomando como referencia el previsto con carácter previo a la aprobación de la citada

[9] Alguna legislación comunitaria ya contemplaba directa o indirectamente la presentación de informes, entre la que destaca: Reglamento 537/2014 de 16 de abril de 2014 sobre los requisitos específicos para la auditoría legal de las entidades de interés público y por el que se deroga la Decisión 2005/909/CE de la Comisión (DO L158/77); Directiva 2014/56/UE, de 16 de abril de 2014 , por la que se modifica la Directiva 2006/43/CE relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas (DO L158/196); Directiva (UE) 2015/849, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n° 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (DO L141/73); Directiva (UE) 2016/943, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L157/1); Reglamento (UE) n° 596/2014, de 16 de abril de 2014, sobre el abuso de mercado y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión (DO L173/1).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

Directiva.[10] Una previsión que actúa a modo de estímulo implícito para que las legislaciones nacionales adopten un marco integral de protección de los denunciantes efectivo.

2.- Retos más inmediatos que plantea la aplicación de la Ley 2/2023 de protección al informante

2.1.- Aspectos clave de la transposición española

En España se presentan pocas denuncias, hay un alto nivel de percepción de la corrupción el nivel de preocupación social por este fenómeno está en claro aumento.[11] Tan es así, que las propuestas de regulación normativa focalizadas en la protección a denunciantes en las pasadas décadas han resultado, a todas luces, testimoniales.[12] El interés por proteger a denunciantes en nuestro país se ha canalizado, mayormente, a través de los conocidos programas de *compliance* destinados para empresas, los cuales han operado a modo de canales informativos tendentes a prevenir situaciones de acoso laboral o por razón de sexo.[13] De hecho, estos se han adelantado a aquellos que han sido impulsados por parte de las administraciones públicas que, como reconoce AMOEDO BARREIRO (2018: 2),

[10] Debe recordarse que, en el año 2019, Transparencia Internacional instó a los países de la UE no solo a respetar, sino también a "reforzar los compromisos de la Directiva a fin de garantizar que la legislación nacional proporcione una protección sólida a todos los denunciantes que informen de infracciones de la legislación nacional o de la UE". Para apoyar tal implementación, elaboró un análisis, que proporciona recomendaciones específicas en el contexto nacional a los efectos de fortalecer la protección de los denunciantes en el proceso de transposición. Transparencia Internacional, *Building on the EU Directive for Whistleblower Protection. Analysis and Recommendations*, 1/2019.

[11] Así, como destaca el último Índice de Percepción de la Corrupción que elabora anualmente Transparencia Internacional, España está empeorando progresivamente en el ranking desde el año 2019 al 2023. Actualmente, consigue una modesta puntuación de 60 puntos sobre 100, situándose en posición 35 de 180 países del mundo. Únicamente están por delante Italia (en posición 41), Polonia (45), Grecia (52), Malta (54), Croacia (57), Rumanía (63) y Bulgaria (72). Transparencia Internacional, Índice de Percepción de la Corrupción (IPC), 2022.

[12] Anteriormente, como examina Rodríguez-Medel Nieto (2019: 238), se había presentado una Proposición de Ley de 17 de enero de 2020, de medidas de lucha contra la corrupción del Grupo Parlamentario Ciudadanos. (Proposición de Ley 122/0000009 de 17 de enero de 2020, de medidas de lucha contra la corrupción), que ya se había registrado en septiembre de 2016 (Proposición de Ley Integral de Lucha contra la Corrupción y Protección de los Denunciantes, 122/000022). Se presentaron enmiendas a la misma por el resto de grupos, aunque su tramitación se bloqueó en la Comisión Constitucional del Congreso de los Diputados. De igual manera, la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales constituye una de las escasas normas que guardan cierto grado de similitud con lo dispuesto en la normativa de protección a las personas informantes.

[13] Sobre la interrelación entre la figura del *whistleblower* y el *compliance* de las personas jurídicas, véase: LEO CASTELA (2021: 47).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

debieron movilizar y gestionar recursos públicos a través de mecanismos tecnológicos y de inteligencia artificial cada vez más sofisticados centrados en la lucha contra la corrupción.

Sin embargo, tras la aprobación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción,[14] aplicable desde el 13 de marzo de ese año, se produce un punto de inflexión en el ordenamiento jurídico español. El sector público cuenta con un marco jurídico novedoso que exige la implementación de tales programas, no solo en el ámbito penal, sino en aquellos relativos a buenas prácticas y que resultan plenamente coherentes con los principios de transparencia e integridad que deben aplicarse para así garantizar el buen funcionamiento de las entidades públicas.

Para conseguir tales objetivos, la Ley 2/2023 no parte desde cero, sino que aprovecha las exitosas medidas proactivas de influencia europea que han resultado de aplicación para la gestión de los fondos europeos en contextos como la detección del fraude, la corrupción, los conflictos de intereses y la doble financiación que se han desarrollado hasta el momento. La Orden estatal HFP/1030/2021, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia constituye buena prueba de ello puesto que en el apartado 2.b.i.A.II del anexo III.C ya incluía referencias a cuestiones reguladas en la actual Ley 2/2013, como ahora los cauces de denuncia. Así pues, la Orden fija como elemento para prevenir la corrupción establecer dichos cauces de denuncia, de manera que opcionalmente las unidades gestoras de las administraciones podrían proveerles entre las medidas de sus planes antifraude para gestionar los fondos europeos derivados de dicho Plan de Recuperación.[15]

No obstante, el nudo gordiano de esta ley se centra en dotar a las personas informantes de un marco normativo que garantice una adecuada protección y confidencialidad, instando a crear un clima de confianza entre estos y la administración que siente las bases de un sistema legal integral de protección al informante (Título VII) en nuestro país. Es más, PAUNER CHULVI (2023: 295) recuerda que, tanto esta ley como la Directiva "mantienen un delicado equilibrio por cuanto ambas tratan de promover las denuncias, atajando las denuncias falsas o malintencionadas y previniendo daños reputacionales injustificados"

Se trata de una novedad en nuestro país que, como se evidencia el preámbulo, se suma a las experiencias previas y más adelantadas de algunas autonomías, que ya

[14] Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

[15] Orden estatal HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia..

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

habían regulado instituciones centradas en recibir comunicaciones de ciudadanos informando de irregularidades[16] a fin de fortalecer la llamada "cultura de la información". Para ello, parte de la premisa de que la colaboración ciudadana constituye un factor esencial para la eficacia del Derecho y que se manifiesta no solo con la sujeción de todos los poderes públicos y de la ciudadanía a la Constitución Española y al resto del ordenamiento jurídico (artículo 9.1 de la Constitución Española), sino con el compromiso colectivo con el buen funcionamiento de las instituciones públicas y privadas. Es más, ésta se proyecta sobre el deber de los trabajadores –y que podría ser extensible, incluso, a cargos públicos electos– de informar o alertar sobre determinadas categorías de irregularidades de las cuales tengan conocimiento en el contexto de su relación laboral o profesional con la finalidad de prevenir y detectar prácticas fraudulentas y corruptas que, en definitiva, amenazan el interés público.

En todo caso, su anclaje normativo supone la culminación del proceso de transposición de la Directiva 2019/1937 al ordenamiento jurídico español[17] el cual se ha producido con notable dilación. Esto no solo ha denotado el escaso interés de nuestras instituciones por consolidar la integridad y la lucha contra la corrupción, sino que tiene lugar como consecuencia de la apertura de un procedimiento de infracción por parte de la Comisión. De tal manera, el 15 de febrero de 2023, esta decidió llevar ante el Tribunal de Justicia de la Unión Europea (TJUE) a varios países –incluido España– por falta de transposición y notificación de las medidas nacionales

[16] El citado Preámbulo reconoce lo siguiente: "(…) las comunidades autónomas de Cataluña, Valenciana, Illes Balears, Navarra, Principado de Asturias o Andalucía han abordado la cuestión de la protección de los denunciantes, si bien la regulación ha sido parcial y centrada fundamentalmente en la creación de oficinas o agencias con la específica función de prevenir e investigar casos de uso o destino fraudulentos de fondos públicos, aprovechamientos ilícitos derivados de actuaciones que comporten conflictos de intereses o uso de información privilegiada, o en general conductas contrarias a la integridad; es decir, han circunscrito esta legislación al ámbito público, con carácter previo en algunos casos a la Directiva 2019/1937".

[17] Un proceso que comenzó el 4 de marzo de 2022, cuando el Gobierno español de manera oficial y por tramitación urgente hizo público el Anteproyecto que buscaba la transposición de la Directiva europea en el ordenamiento jurídico español. Acto seguido, el 13 de septiembre de 2022 el ejecutivo anunció la aprobación del Proyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, que se publicó el 23 de septiembre de 2022 a su anuncio por el Consejo de Ministros, y fue remitido a las Cortes Generales para su tramitación. Este introdujo no únicamente modificaciones en la depuración de su redacción, sino también novedades relevantes, tales como la ampliación del ámbito subjetivo de la norma, la ampliación del plazo máximo de instrucción y una nueva regulación de la Autoridad Independiente de Protección al Informante. Tras la fase legislativa ante el Senado, el 21 de febrero, se publicó en el BOE la Ley 2/2023, de 20 de febrero reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

de transposición de la Directiva.[18] A ello se le adhiere el pronunciamiento dimanante de la STJUE en el asunto C-658/19, de 25 de febrero de 2021, en el que Tribunal expresó taxativamente la falta de diligencia del legislador español y la especial gravedad del retraso como obstáculo al correcto funcionamiento del espacio de libertad, seguridad y justicia dentro de la Unión.[19]

Así, pese a que parecía que la demora considerable de varios Estados miembros en la transposición era el motivo principal a la hora de que la Comisión iniciara un procedimiento formal de infracción, lo cierto es que ha ido más allá y recuerda que va a prestar especial atención a la forma en la cual se está realizando la adaptación nacional. Por lo que concierne a España, la Ley 2/2023 conlleva importantes novedades fruto de la especificación nacional en transposición de la Directiva y que deben citarse sucintamente.

En cuanto al Título II de esta ley (arts. 4 y siguientes), se establece la obligación tanto para empresas como para el sector público de contar con un sistema interno de información completo compuesto tanto del habitual canal de comunicación –conocido, comúnmente como canal ético o de denuncias–, como del proceso de

[18] Ya el Grupo de Estados contra la Corrupción del Consejo de Europa (GRECO) había advertido en su informe del año 2021 de que España carecía de una legislación adecuada de protección de los denunciantes (Grupo de Estados contra la corrupción, *Quinta ronda de evaluación. Prevención de la corrupción y promoción de la integridad en gobiernos centrales (altas funciones ejecutivas) y las fuerzas y cuerpos de seguridad.* Adoptado por GRECO en su 88a reunión plenaria, Estrasburgo, 20-22 septiembre 2021, p. 18. (ref. GRECORC5(2021)8). Así, en enero de 2022, la Comisión envió cartas de emplazamiento a 24 Estados miembros –incluido España– por no transponer completamente e informar a la Comisión de las medidas de transposición antes de la fecha límite. En el caso de nuestro país, inició este procedimiento de infracción contra España (INFR(2022)0073) aunque, tras la respuesta de las autoridades españolas, emitió un dictamen motivado en julio de 2022 advirtiendo del compromiso de garantizar la aplicación de la Directiva de la UE sobre denunciantes. Respuesta del Sr. Reynders en nombre de la Comisión en el Parlamento Europeo (pregunta parlamentaria núm. E-002602/2022(ASW)). Además, en julio de ese mismo año, la Comisión envió dictámenes motivados a 15 Estados miembros y a cuatro Estados miembros en septiembre de 2022 por no comunicar las medidas de transposición íntegra de la Directiva. Las respuestas de ocho Estados miembros –incluido España– a los dictámenes motivados de la Comisión no fueron satisfactorias, razón por la que la Comisión decidió el 15 de febrero de 2023 llevar a estos Estados miembros ante el TJUE. Comisión Europea, *La Comisión Europea decide llevar a 8 Estados miembros al Tribunal de Justicia de la Unión Europea por la protección de los denunciantes*. Comunicado de prensa, 15 de febrero de 2023.

[19] Para un análisis de la citada STJUE, remitimos al siguiente comentario: NAVARRO MEJÍA (2021: 611-628).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

gestión y seguimiento de la información recibida.[20] Precisamente, es más que evidente que este sistema debería emplearse de manera preferente para canalizar la información aunque el informante puede elegir el canal interno o externo, según las circunstancias y riesgos de represalias que pueda considerar.

Asimismo, las entidades deberán designar un responsable del sistema interno de información (arts. 5 y 8) que podrá ser una persona o un órgano colegiado y cuyo nombramiento, destitución o cese dependerá del órgano de administración o gobierno de la entidad. La gestión del sistema puede ser interna o externa a la entidad (art. 12). En el caso de que se externalice la gestión, deberán respetarse las garantías previstas en la ley y la responsabilidad, en todo caso, recaerá igualmente en el responsable del sistema que se haya nombrado en la entidad (arts. 6 y 8). El canal de comunicación que forma parte del sistema debe permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas, por medios electrónicos o, incluso, de forma presencial (arts. 5 y 7). Las comunicaciones por el canal serán confidenciales (art. 5.2º b) y deberán permitir también que se presenten o tramiten posteriormente comunicaciones anónimas (art. 7.3º). Asimismo, el procedimiento de gestión de las informaciones responderá al contenido mínimo y principios previstos en el art. 9 de esta ley.[21]

En relación con el Título III (arts. 16 y siguientes), se regula el canal externo de información, de manera que el informante puede optar por informar a la Autoridad Independiente de Protección del Informante (en adelante, AIPI) o a las autoridades u órganos autonómicos competentes, ya sea directamente o previa comunicación a

[20] Estarán obligadas a disponer de dicho sistema interno de información: a los tres meses desde la entrada en vigor de la Ley, esto es, el 13 de junio de 2023: las entidades del sector público salvo los municipios de menos de 10.000 habitantes, las entidades jurídicas del sector privado de 250 o más trabajadores o los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos. En caso de que se trate de entidades jurídicas del sector privado de entre 50 y 249 trabajadores o municipios de menos de 10.000 habitantes, ven alargado este plazo hasta el 1 de diciembre de 2023.

[21] Entre estos, destaca la obligación de a)"acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción"; b) "determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación" o f) "el establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

través del correspondiente canal interno22. Es más, como recuerda SIERRA RODRÍGUEZ (2023: 100-101), esta Autoridad "debería ser la que impulse el cumplimiento de la Ley y coordine el ecosistema multinivel que actúa en esta materia. Sin embargo, la norma no es expresa en estos términos y ha sido extremadamente cautelosa sobre el desempeño de esta función que queda implícita y atenuada, aunque sea evidente que tiene las atribuciones más relevantes por su especialización y por el alcance territorial de sus competencias respecto a las alertas, protección y sanciones". Es más, en última instancia, el informante podrá hacer una revelación pública de la infracción de la que ha tenido conocimiento, tras haber realizado la comunicación primero por canales internos y externos, o directamente, por canales externos –siempre que no se hayan tomado medidas apropiadas al respecto en el plazo establecido y entienda que se da una situación de peligro inminente para el interés público, entre otros–.

No menos baladí es el establecimiento de un preciso régimen sancionador,[23] que contempla elevadas cuantías de multas tanto para la entidad infractora, pública o privada, como para los órganos internos responsables. Así, según lo dispuesto en el art. 65, parten de 1.001 hasta 300.000 euros en el caso de las personas físicas y entre 100.000 y el millón de euros si las que cometen una infracción son personas jurídicas, intervalos que oscilan en función de su gravedad. En cualquier caso, para el caso de las muy graves, se prevé igualmente a) la amonestación pública; b) la prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años y; c) la prohibición de contratar con el sector público durante un plazo máximo de tres años. En definitiva, pese a que el régimen sancionador incentivará que las empresas se adapten lo antes posible a las novedades previstas en esta ley, deja a éstas en una situación complicada, puesto que deben cumplir con sus obligaciones legales en un tiempo récord so pena de altas sanciones que pueden llegar a comprometer su viabilidad.

Con todo, en virtud del art. 61 de la Ley 2/2023, el órgano sancionador nacional se confiere a la AIPI, que todavía no ha sido creado. Si bien, para el caso de las comunidades autónomas, Cataluña se adelanta y se sitúa a la vanguardia de España, pues ya ha conferido tal competencia a su Oficina Antifraude. Se trata así de la primera autoridad independiente que asume plenas competencias para la

[22] Informar sobre una irregularidad a una autoridad independiente, sea estatal o autonómica, supone, como apunta CLEMENTE MARTÍNEZ (2022: 136) cumplir también con el deber de actuación que prevé la normativa sobre buen gobierno, lo que además implica un acto de valentía de los dirigentes que lo llevan a cabo. Sobre la noción del concepto de independencia aplicable –por analogía– a las autoridades de protección de datos, remitimos al siguiente estudio: GARCÍA MAHAMUT (2023: 179-199).

[23] El art. 63 contempla las definiciones de infracciones muy graves, graves o leves.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

protección de las personas informantes, tanto en lo relativo a la previsión de canales externos como en el empleo inminente de la potestad sancionadora.[24]

2.2.- Cuestiones más problemáticas de la Ley 2/2023 de protección de las personas informantes

Al margen de las novedades más destacadas que la Ley 2/2023 incorpora al ordenamiento jurídico español anteriormente citadas, es innegable que su aprobación ha evidenciado un deficitario trámite parlamentario que, en buena medida, se aprecia a través de un cierto grado de desorden en la configuración de la norma en varias de sus disposiciones, lo que ya está generando efectos adversos para distintos operadores jurídicos. Por lo pronto, toda vez que España ha cumplido con la transposición de la Directiva europea, en este apartado trataremos de sintetizar aquellas disposiciones que, o bien adolecen de la suficiente eficacia o bien, plantean problemas de encaje constitucional sobre su compatibilidad con otra legislación estatal tanto de carácter general como sectorial.

En primer lugar, cabe destacar que, aunque la ley apuesta fielmente por eliminar cualquier referencia negativa mediante el empleo general del término informante reemplazándola por su conceptualización como "informante" –ello, en una clara apuesta por alejarse del término "denunciante" prefijado inicialmente en las disposiciones de la Directiva y que tantas connotaciones negativas ha tenido a lo largo de las pasadas décadas en nuestro país–, no hay género de duda el descuido de nuestro legislador de incluir, por su actuación apresurada, aquellas referencias expresas –a la par que testimoniales– al concepto de "denunciante".[25]

En segundo lugar, no debe pasarse por alto uno de los preceptos más característicos que evidencian una técnica legislativa imprecisa y que parte del propio tenor literal del art. 9.2 j) de la Ley 2/2023, cuya interpretación literal podría entrar en directa colisión con el derecho de defensa de las empresas. Esta disposición establece el contenido mínimo y principios que debe reunir el procedimiento de gestión de informaciones susceptibles de aprobación por los respectivos órganos de administración de las empresas obligadas, para lo que prevé la "remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito". En este sentido, de esta disposición parece desprenderse un deber inexcusable de remitir los hechos a la Fiscalía, en vez de contemplar la mera posibilidad para aquellos sujetos obligados. Y ello no solo

[24] Estas nuevas competencias son una realidad tras su aprobación en la Ley de acompañamiento de los presupuestos de la Generalitat de 2023. Disposición adicional séptima. 1 de la Ley 3/2023 de la Generalitat de Catalunya, de 16 de marzo, de medidas fiscales, financieras, administrativas y del sector público para el 2023.

[25] Véase, a modo de ejemplo, el apartado 3º del preámbulo de esta Ley o el art. 4.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

DOI: https://doi.org/10.51915/ret.313

sobre la base de la inmediatez, sino también partiendo de hechos sobre los que únicamente se exigen indicios en lugar de que éstos sean constitutivos de un delito.

En efecto, de esta disposición parece entenderse que el responsable del sistema interno de información, tras la comunicación de denuncia, deberá remitir tales hechos al Ministerio Fiscal *ipso facto*. Tal exigencia con ausencia de deber de investigarlos a fin de comprobar o verificar la existencia de verosimilitud podría tener efectos adversos para la organización o empresa afectada que, a la postre, podría vulnerar el derecho de defensa. En consecuencia, si bien la Ley 2/2023 pretende fomentar los programas de *compliance* implementados por las organizaciones a través de los canales internos de información, estos no deberían canalizarse a través de la obligación de autodenuncia ante el Ministerio Fiscal. En este caso, ésta adolecerá de la suficiente garantía de protección para las organizaciones frente a aquellas imputaciones que no acrediten fehacientemente la presunta comisión de determinados delitos por parte de su personal directivo o empleado.

En tercer lugar, emergen serias dudas sobre la interrelación entre esta norma con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)[26] o, incluso, lo que podría derivarse en una posible incompatibilidad entre ambas. Al efecto, la previsión del art. 11 de la Ley 2/2023 por la que faculta para el libre intercambio de información a través de canales de grupos de sociedades[27] entra en directa contradicción con el deber de transparencia e información al afectado del art. 11 LOPDGDD y con el principio de limitación de la finalidad, un principio vertebrador de la normativa de protección de datos que restringe la cesión o comunicación entre empresas de determinados datos de carácter personal.

De esta manera, con carácter previo a la aprobación de la normativa de protección de informantes, el art. 64 de la Ley 9/2017 sobre Contratos del Sector Público (LCSP) ya imponía a los poderes públicos el deber de implantar aquellas medidas de prevención y control que impidan situaciones de corrupción, favoritismo o fraude y prevenir, detectar y solucionar de forma efectiva todo conflicto de interés que pueda

[26] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[27] Tal posibilidad se prevé expresamente por el apartado 3º del art. 11 que contempla lo siguiente: "Será admisible el intercambio de información entre los diferentes Responsables del Sistema del grupo, si los hubiera, para la adecuada coordinación y el mejor desempeño de sus funciones".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

surgir en los procedimientos de licitación[28]. Incluso, otra legislación sectorial ha excedido de este cometido, previendo cauces de denuncia anónimas cuyos efectos positivos son incuestionables, tal y como reconoce un amplio sector doctrinal,[29] aunque, correlativamente, también incremente el riesgo a la presentación de denuncias de mala fe.[30] Este es el supuesto de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo[31] o la relativa a la protección de datos anteriormente citada. Esta última merece especial énfasis ateniendo a su directa relación con la Ley 2/2023, pues el art. 24 de la LOPDGDD ya preveía la creación y mantenimiento de sistemas de información a través de los cuales se puede comunicar a una entidad de Derecho privado, incluso anónimamente, la

[28] Resulta reseñable cómo la Ley 2/2023 modificó el art. 71.1.b) LCSP incluyendo entre las prohibiciones para contratar las de entidades que hubieran sido sancionadas por infracciones muy graves de la Ley 2/2023; si bien, a raíz de la Ley 4/2023, de 28 de febrero, para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI se ha suprimido dicha referencia al añadir como una prohibición de contratar las entidades que vulneren dicha Ley 4/2023. Se trata éste de un error legislativo que deberá ser subsanado (así lo advierte VÁZQUEZ MATILLA, J., "Incidencias en contratación: Ley 4/2023, de 28 de febrero, para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI, *Blog de Javier Vázquez Matilla,* 2023) para cumplir con el citado art. 64 LCSP, ya que, sin duda, una forma de prevenir la corrupción en las administraciones es, precisamente, evitar la contratación de empresas que hayan incumplido la normativa de protección de informantes, ya que podrían acabar actuando de forma no ética con la administración que les quisiera contratar debido a su historial incumplidor en la materia. (Pendiente actualización mayo 2023).

[29] Frente a la discrecionalidad de los Estados miembros para contemplar la posibilidad de admitir denuncias anónimas, se posiciona AMOEDO BARREIRO (2017: 7). Así, como afirma VESTRI (2019: 21) el anonimato constituye una de las medidas más eficaces de protección frente a las personas informantes. En palabras de ALIAGA RODRÍGUEZ (2022: 67), el anonimato es esencial no solo desde la óptica del informante, que se asegura de forma efectiva a auto protección frente a posibles represalias que se pudieran adoptar contra él, sino también desde el interés de las organizaciones, que ven un incentivo real en la suministración de información necesaria para detener o evitar irregularidades. Aunque para ello, como expone SIERRA RODRÍGUEZ (2020: 38), resulta indispensable que el informante pueda realizar un seguimiento real a fin de que pueda conocer de primera mano el desenlace de las alertas que ha efectuado.

[30] En definitiva, como reconoce GARRIDO JUNCAL (2019: 137), aquellas que contienen información falsa, tergiversada u obtenida de forma ilícita, así como aquellas "que se presentan con el mero propósito de difundir el descrédito y la difamación de la persona a la que vayan referidas".

[31] Los arts. 26 bis. y 63 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo prevé que los empleados, directivos o agentes informen sobre infracciones de esta Ley. En estos supuestos, los sujetos informantes pueden formular denuncias anónimamente mediante canales internos o externos y los sujetos obligados deben velar por el cumplimiento de las normas de protección de datos, así como asegurar que los informantes no sufran represalias.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

comisión en su seno o por terceros, de conductas contrarias a la normativa general o sectorial que le sea aplicable.

En este punto, ha llamado la atención que este precepto –previsto en esta ley orgánica– haya sido modificado por la disposición final séptima de la Ley 2/2023, lo que ha generado dudas de calado sobre la supuesta transgresión del principio de reserva de ley[32], Sin embargo, el art. 24 de la LOPDGDD tiene carácter ordinario (no orgánico) a tenor de la Disposición final primera de esta ley, por lo que tal previsión no transgrede tal principio. Ello, con independencia de que quizá hubiera resultado más apropiado y pertinente una modificación directamente en la LOPDGDD al tratarse de la norma medular que, hasta la fecha, ha regulado los sistemas de información de denuncias internas y respecto a los cuales ya se disponía la posibilidad de presentar denuncias anónimas, así como la necesidad de preservar y proteger la identidad de la persona denunciante en caso de que se hubiera identificado–.

En otro orden de cosas, resulta relevante poner de manifiesto la incongruencia existente entre el preámbulo de la Ley y su articulado en relación con el Delegado de Protección de Datos (DPD). A este respecto, el propio apartado 3º del preámbulo contempla expresamente: "se exige que las entidades obligadas a disponer de un Sistema interno de información, los terceros externos que en su caso lo gestionen y la Autoridad Independiente de Protección de Datos, A.A.I., así como las que en su caso se constituyan, cuenten con un delegado de protección de datos".

De la propia redacción de este precepto, la obligación de contar con un DPD parece extenderse a cualquier entidad obligada que disponga de un sistema interno aunque, posteriormente, el propio art. 34 de la ley únicamente exige nombrar un DPD a la AIPI y a las restantes autoridades independientes autonómicas análogas a ésta última. Dicho lo cual, entendemos la prevalencia de tal precepto frente a lo dispuesto en el preámbulo, por lo que la exigencia de contar con un DPD deberá extenderse a toda autoridad independiente a lo que se adicionarán aquellos responsables y encargados del tratamiento que cuentan con tal obligación según lo dispuesto en la LOPDGDD. Por último, nada obsta al resto de responsables y encargados del tratamiento para que cuenten con esta persona física o jurídica independiente –encargada de informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos– tras la implementación de sus respectivos sistemas internos de información, pues tal

[32] Para tal fin, nos hacemos eco de afirmaciones recientes como la que realiza Javier Puyol, magistrado en excedencia y ex letrado del Tribunal Constitucional en un reciente blog de la revista Economist & Jurist, en el que el 13 de marzo de 2023 apuntaba expresamente lo siguiente: "(…) la Disposición Final Séptima de esta ley modifica el artículo 24 de la Ley Orgánica 3/2018 de Protección de Datos. Es curioso que una ley ordinaria modifique preceptos de una Ley Orgánica".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

designación fomenta el fiel respeto de la normativa de la protección de datos vigente.[33]

De lo anteriormente expuesto, es más que evidente que la Ley 2/2023 no es estrictamente de índole administrativa, pues su aplicabilidad se hace extensible tanto para el sector público como para el privado. Ahora bien, dispone de una especial incidencia en el ámbito público, por cuanto desplaza a la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC) —la cual exige la identificación de la persona que informa sobre una infracción, lo que impide *de facto* la presentación de denuncias anónimas— mediante el reconocimiento para un sujeto de informar anónimamente o no sobre una infracción.

Por último, cabe preguntarse qué va a suceder con aquellas comunidades autónomas que no tienen una agencia antifraude autonómica. En este sentido, cabe preguntarse si sería viable, por ejemplo, que estas optaran por atribuir más competencias al Defensor del Pueblo autonómico.

En la actualidad, parece que solo hay dos alternativas para poner en funcionamiento el canal externo: o bien, las agencias antifraude autonómicas –actualmente, España cuenta con 5: la Oficina Antifrau de Catalunya; la Oficina de Prevención y Lucha contra la Corrupción de la Islas Baleares; la Oficina Andaluza contra el Fraude y la Corrupción; la Oficina de Buenas Prácticas y Anticorrupción de Navarra y la Agencia

[33] El art. 34 de la Ley 2/2023 remite a lo dispuesto en el art. 37.1.a) del Reglamento General de Protección de Datos, en lugar de remitir directamente a la LOPDGDD que, en su art. 34 (apartado primero) concreta aquellos responsables y encargados del tratamiento cuya designación de un DPD resulta preceptiva. Por su parte, en el segundo apartado se contemplan "otros" responsables o encargados del tratamiento, en cuyo caso, la designación de tal designación resulta, evidentemente, facultativa.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

Valenciana Antifraude–[34] o bien, la futura AIPI estatal.[35] La delegación competencial a los Defensores del Pueblo autonómicos podría erigirse como cauce legal efectivo para conferir a estas instituciones las funciones análogas asumidas por las agencias antifraude autonómicas. Si bien, en este caso, convendría revisar el tenor literal de los Estatutos de Autonomía para precisar si éstos deben reformarse a fin de prever a estos altos comisionados de las asambleas de las comunidades autónomas funciones de la AIPI estatal en el ámbito autonómico –en todo caso, deberá procederse a la reforma de las leyes que lo desarrollen a fin de contemplar las funciones que les son propias–.

Una ampliación competencial que, en el caso de producirse, incrementaría sustancialmente no únicamente la homogeneidad en las actuaciones administrativas –en tanto en cuanto, tales funciones serían asumidas por los defensores de pueblo autonómicos que, en líneas generales cuentan con una estructura administrativa semejante–, sino también la eficiencia en la implantación de los sistemas de protección de informantes. Y ello, desde dos perspectivas distintas: la primera, habida cuenta de que no sería necesario crear una autoridad independiente *ad hoc* en aquellas comunidades autónomas que no cuentan con una agencia antifraude y, la segunda, por cuanto proporcionaría una respuesta más próxima a la ciudadanía informante en tiempo y forma, lo cual resulta especialmente relevante teniendo en cuenta las represalias a las que pueden verse sometidos.

3.- La aplicación material y personal de la Ley 2/2023: algunos aspectos críticos

Como trataremos de analizar a continuación, pese a que la Ley 2/2023 excede de un mero marco normativo de protección del denunciante hacia una ampliación del

[34] Además, Aragón cuenta con la Agencia de Integridad y Ética Públicas, que fue creada en virtud de la Ley 5/2017, de 1 de junio, de Integridad y Ética Públicas aunque no cuenta con actividad relevante. También Asturias ha contemplado el Canal de Lucha contra la Corrupción, a modo de buzón de denuncias, dentro del Portal de Transparencia de la Administración del Principado de Asturias, cuya gestión se encomienda a la Oficina de Buen Gobierno y Lucha contra la Corrupción en virtud de la Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés. Todo ello, sin perjuicio de las agencias municipales que fueron creadas a nivel municipal en Madrid y Barcelona. (El Pleno del Ayuntamiento de Madrid aprobó, en sesión celebrada el 23 de diciembre de 2016, el Reglamento Orgánico de la Oficina Municipal contra el Fraude y la Corrupción, y dicha Oficina Municipal está operativa desde octubre de 2018 una vez nombrado su Director, el resto del personal, adjudicarle una sede y contar con su Registro y sistema de gestión informático; la Comisión de Gobierno del Ayuntamiento de Barcelona, por acuerdo de 29 de diciembre de 2015, aprobó la creación de la Oficina para la Transparencia y las Buenas Prácticas).

[35] BUENO SÁNCHEZ (2022: 209-240) descarta acudir a otros órganos, a pesar de que la Directiva abría esa posibilidad al disponer en su art. 11 la obligación activa general de los Estados miembros de designar "a las autoridades competentes" en el establecimiento de denuncia externa y de seguimiento de las mismas.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

ámbito material y personal de la Directiva, esta puede catalogarse de confusa y disfuncional en aspectos clave que, en determinados contextos, podría vaciar de efectividad la normativa europea de referencia. Como analizaremos a continuación, esto ha lastrado considerablemente una de las principales oportunidades con la que contaba el legislador español, en esencia, la clara aspiración de "que el derecho interno vaya más allá y se amplíen los ámbitos de aplicación personal y material, las garantías y las protecciones que se configuran como mínimas" (SIERRA RODRÍGUEZ: 2020: 82).

3.1.- El ámbito de aplicación material u objetivo

Como consecuencia de las competencias limitadas de la UE, el ámbito de aplicación material de la Directiva resulta sumamente fragmentado, complejo y, a todas luces, restringido por cuanto simplemente protege a los informantes que denuncian infracciones de la legislación de la UE en áreas muy definidas. De hecho, el art. 2 de la Directiva define el ámbito material a través de conceptos abstractos como los intereses financieros de la UE (apartado 1 letra b)[36] y el mercado interior (apartado 1 letra c), para lo cual remite a su Anexo que, en su Parte II contempla un listado extenso de actos de la UE. En su apartado 1º prevé la existencia o sospecha razonada y fundada de cualquier infracción del Derecho de la UE y que, como reconoce MIRANZO DIAZ (2019: 373), "busca desincentivar el torpedeo malintencionado de las decisiones o las meras venganzas personales".

El problema radica en que, si estos deciden denunciar infracciones[37] tanto de otras áreas de la legislación de la UE como aquellas de índole nacionales que no se encuentran claramente definidas en la legislación del Estado miembro en cuestión, no estarán amparados por la protección conferida por la legislación de protección al denunciante. Un déficit normativo que resulta especialmente preocupante por cuanto puede entrar en directa contradicción con el primer párrafo del art. 6.1 a) de la Directiva, que exige como condición para conferir protección que los

[36] Los intereses financieros de la UE se prevén en el art. 2.1 del Reglamento 883/2013 y abarcan tanto los ingresos, gastos y activos cubiertos por el presupuesto de la Unión Europea, como los presupuestos de las instituciones, órganos, oficinas y agencias y los presupuestos gestionados y controlados por ellos.

[37] La infracción es, ciertamente, un concepto flexible por cuanto abarca también la "información sobre infracciones", tanto aquella relevante, como *"(…) las sospechas razonables, sobre infracciones reales o potenciales, que se hayan producido o que muy probablemente puedan producirse en la organización en la que trabaje o haya trabajado el denunciante o en otra organización con la que el denunciante esté o haya estado en contacto con motivo de su trabajo, y sobre intentos de ocultar tales infracciones"* (art. 5.2). En caso de alcanzar dicho umbral, el denunciante ostenta la protección frente a cualquier tipo de acoso. De hecho, la Directiva prohíbe cualquier acto u omisión que cause un perjuicio, ya sea directo, indirecto, se trate de amenazas o tentativas de represalias, acto realizado, instado o simplemente tolerado (art. 19 de la Directiva contempla la amplia amalgama de represalias proscritas).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

denunciantes no solo "tengan motivos razonables para pensar que la información sobre infracciones denunciadas es veraz en el momento de la denuncia (…)" sino que, además, la información entre "dentro del ámbito de aplicación de la presente Directiva". Por lo tanto, la denuncia de infracciones estará o no protegida en función de la materia susceptible de divulgación, razón por la que concurre un interés esencial en la necesidad de delimitar el ámbito de aplicación material previsto por la ley 2/2023 para así determinar si la persona informante recibirá o no protección frente a posibles represalias.[38]

Indudablemente, el mero mantenimiento del enfoque de la Directiva en sede nacional hubiera dejado a muchos denunciantes desprotegidos, estos no tendrían plena certeza sobre qué comportamiento a la hora de informar se ajusta a los criterios legales establecidos y conduciría, en última instancia, a situaciones en las que las personas deciden no hablar, o ante la creencia errónea de que están protegidos, son vulnerables a represalias.[39] Máxime cuando la Directiva no limita el alcance material en sede nacional por cuanto subraya la posibilidad de que los Estados miembros amplíen "la protección en su Derecho nacional a otros ámbitos o actos (…)" con el fin de garantizar que haya un marco integral y coherente de protección de los denunciantes en el ámbito nacional (art. 2.2 y Considerando 5). Es más, la Comisión Europea alentó a hacerlo, reconociendo que "un enfoque integral es indispensable para reconocer la contribución significativa de los denunciantes para prevenir y combatir conductas ilícitas que perjudiquen el interés público, y para garantizar que estén debidamente protegidos en toda la UE".[40]

Precisamente, el art. 2 de la Ley 2/2023 ha seguido este enfoque y su ámbito de aplicación material se centra en la protección de las personas que, en un ámbito laboral o profesional, detecten infracciones de la normativa de la UE. Si bien, va más allá pues también posibilita la comunicación a través de los mecanismos previstos formalmente de cualquier infracción penal o administrativa grave o muy grave de nuestro ordenamiento jurídico –en todo caso, se incluyen aquellas que conllevan un

[38] Recordemos que, en caso de que esté dentro del ámbito de aplicación material, en ningún caso resultará gradual, sino que la protección se extenderá directamente sobre toda represalia, de manera que los Estados miembros deberán responder contundentemente mediante sanciones ya sea de índole penales, civiles o administrativas (Considerando 102).

[39] Cabe destacar que los estándares internacionales adoptados por Transparencia Internacional recomendaban que la legislación sobre denuncias debería disponer de un alcance material lo suficientemente amplio y claro a fin de que cubra la gama más extensa posible de irregularidades. Transparencia Internacional, *Principios Internacionales para la Legislación de Denunciantes*, 2013, p. 4; Proyecto de Responsabilidad Gubernamental (GAP), *Políticas sobre Mejores Prácticas Internacionales para Denunciantes,* 22 de julio de 2016.

[40] Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, Reforzar la protección de los denunciantes a nivel de la UE, COM (2018) 214 final.

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

perjuicio económico para la Hacienda Pública y para la Seguridad Social–. Así, aunque la citada Ley pretende fomentar la transparencia, únicamente ampara la denuncia de tales infracciones a través de canales internos y externos de información, lo que llevará a que estos concentren la práctica totalidad de su actividad investigadora sobre aquellas vulneraciones que afecten con un mayor impacto al conjunto de la sociedad.

Sin embargo, correlativamente, dejará fuera un sinfín de otras conductas habituales como puede ser el incumplimiento de las políticas internas y los códigos éticos de las organizaciones u otros comportamientos vinculados con el abuso de poder. Este enfoque podría vaciar de protección las garantías predefinidas por la Directiva, habida cuenta de que la finalidad de esta radica en comprender áreas en la que se producen situaciones de acoso, abusos de autoridad o cualquier acción u omisión que se produzca en el seno de una organización pública o privada que, en definitiva, frustre el objetivo de denunciar cualquier información que contraríe el interés público general de la UE y nacional.

Es innegable que tal ausencia –y por ende, de aparente exclusión– en la Ley 2/2023 supone la desprotección de conductas relevantes y cotidianas como el *dumping* salarial o la discriminación laboral que, por el contrario, si que contemplan directa o indirectamente otras legislaciones nacionales de nuestro entorno como es el caso de la legislación francesa, en virtud de la aplicación de la actual Ley núm. 2022-401 (conocida como "Loi Waserman").[41]

Por añadidura, el apartado 2º del citado artículo dispone que la previsión de que la protección que confiere la norma no excluye la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación. Una disposición que, igualmente, se diferencia de la Ley francesa núm. 2022-401 que, en su art. 10-1.-I, otorga inmunidad –incluyendo responsabilidad penal y civil– a la persona informante. Y, pese a esta disposición encaja coherentemente con la posibilidad que contempla el art. 21.3º de la Directiva que dispone que los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente "siempre que dicha adquisición o acceso no

[41] Francia, pese a que ya contaba con medidas integrales de protección de denunciantes desde 2016 conforme a la Ley Sapin II, la Ley 2022-401 de 21 de marzo de 2022 destinada a mejorar la protección de los denunciantes, resulta más garantista. En efecto, el alcance material ampara toda denuncia que lesione el interés general nacional o comunitario, en particular cuando exista una situación de emergencia o riesgo de lesión irreversible (art. 6 salvo las excepciones del art. 8). Ley n° 2022-401 de 21 de marzo de 2022 destinada en mejorar la protección de los denunciantes. JORF n°0068 de 22 de marzo de 2022 (NOR : JUSX2132193L). Véase igualmente el Decreto núm. 2022-1284 del 3 de octubre de 2022, por el que implementa la Ley francesa n° 2022-401 de 21 de marzo de 2022, sobre la protección de los denunciantes, que entró en vigor el 4 de octubre de 2022.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

constituya de por sí un delito", podría tener un efecto disuasorio considerable entre posibles informantes.

En esta línea, casos tan sonados como los relativos a los delatores del escándalo LuxLeaks Antoine Deltour y Raphaël Halet, trabajadores de la consultora PwC y que filtraron miles de documentos que evidenciaban las ventajas fiscales concedidas por el Gran Ducado a multinacionales, no estarían protegidos por la ley española. Cuestión, a todas luces, incongruente, considerando que este caso tan mediático propiciaría la adopción de la (entonces) propuesta de Directiva.

Que la Ley 2/2023 no exima de responsabilidad penal a las personas que informen de casos de corrupción constituye un déficit importante en nuestro sistema democrático por cuanto supone la desprotección de potenciales informantes que ayudarían a destapar casos de perjuicios de primer orden para el interés público. En nuestro país, este sería el caso de la persona que hizo públicos los correos electrónicos de Blesa que demostraban la existencia de las "tarjetas *black*", que no estaría protegido si hubiera denunciado o revelado públicamente la información –únicamente si hubiera informado de forma anónima y bajo su propio riesgo–. Así se contempla por el art. 35 de la citada ley, que extiende la protección contra represalias a una ulterior identificación solo para los casos en los que, además de que el sujeto en cuestión hubiera tenido "motivos razonables para pensar que la información referida es veraz", esta debe –en todo caso– entrar "dentro del ámbito de aplicación de esta ley".

Parece que la nueva ley no toma conciencia de los casos que mayor repercusión pública han tenido a escala mundial en la última década, como la mayor filtración de inteligencia en la historia de la Agencia de Seguridad Nacional de los Estados Unidos –en el año 2013, el consultor tecnológico Edward Snowden destapaba el espionaje masivo realizado por esta Agencia– o el papel fundamental que jugó Hervé Falciani a la hora de destapar a evasores fiscales en todo el mundo –y que lleva desde el año 2009 colaborando con la justicia de varios países para relevar a evasores fiscales que guardan su dinero en bancos suizos–.

Lo que está claro es que la Ley 2/2023 no sigue a las legislaciones nacionales más garantistas como Francia, donde incluso su legislación de protección de denunciantes anterior a la transposición de la Directiva, esto es, la conocida como Ley Sapin II, ya preveía la exención de responsabilidad penal de un denunciante que violaba la obligación de secreto protegido si tal divulgación resultaba necesaria y proporcionada para proteger los intereses en juego. Incluso la vigente Ley francesa núm. 2022-401 resulta todavía más garantista, pues amplía el alcance de esta falta de responsabilidad penal, de modo que el denunciante no es responsable penalmente en los casos en los que sustraiga, malverse u oculte documentos o cualquier otro soporte que contenga información de la que tenga conocimiento

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

legítimo. Los tribunales que juzguen tales situaciones comprobarán, por tanto, la proporcionalidad y la necesidad de la infracción cometida a los efectos del ejercicio del derecho de alerta.

3.2.- El ámbito de aplicación personal o subjetivo

La Directiva define *whistleblower* como "una persona física que comunica o revela públicamente información sobre infracciones obtenida en el contexto de sus actividades laborales" (art. 5.7) y que "desempeña un papel clave a la hora de descubrir y prevenir esas infracciones y de proteger el bienestar de la sociedad" (Considerando 1). En efecto, pretende abarcar dentro de esta figura a una gran colectividad de sujetos, comprendiendo a los trabajadores, voluntarios y trabajadores en prácticas, funcionarios públicos, accionistas y a otros miembros del órgano de administración o dirección de una empresa, incluidos los miembros no ejecutivos o cualquier persona que trabaje bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores. Es por ello por lo que provee una definición amplia en la que, indudablemente, deja cabida a que las legislaciones nacionales puedan contemplar sujetos provenientes de un sinfín de sectores, incluido aquellas organizaciones sin ánimo de lucro.

Un "tercer" sector, este, que España no contempla en la Ley 2/2023, lo que supone una oportunidad regulatoria perdida de protección a estos colectivos. De tal modo, el art. 3 de esta ley protege a las personas informantes que trabajan "en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional" y las denuncien a través de los canales previstos legalmente. Se aplica, incluso, a una relación laboral finalizada, así como a voluntarios, becarios, trabajadores en periodos de formación o aquellos que se encuentren en el proceso de selección o negociación precontractual.[42] Por su parte, llama particularmente la atención la ausencia de elementos medulares, como la

[42] Lo particularmente relevante es la determinación exhaustiva de aquellas personas a las que se les puede conferir protección contra potenciales represalias, estableciendo medidas de protección que no se limitan a aquellos sujetos que hayan realizado una denuncia, sino que se extiende a toda persona física y jurídica que corre el riesgo de recibir un trato injusto como consecuencia de haber denunciado irregularidades. De ahí que los apartados 3º y 4º prevean una multiplicidad de sujetos relacionados con las personas informantes a los que pueden extenderse medidas destinadas su protección contra represalias, incluyendo a representantes legales que asesoran y apoyan al informante, personas físicas que lo asisten o están relacionadas (amistades, familiares, allegados), así como personas jurídicas empleadoras o en las que ostente una participación significativa, esto es, una "participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

necesidad de que el informante divulgue la información de buena fe[43] como condición indispensable para garantizar su protección o, lo que resulta más importante, la ausencia de compensación económica directa.

Por lo tanto, a partir de la entrada en vigor de esta ley, las personas informantes ya no deben ser simplemente sujetos "desinteresados" sino que, con carácter general, tampoco deberán recibir "compensación financiera directa". Así se prevé por el art. 37.1 d) de la Ley 2/2023, que otorga a la futura AIPI la posibilidad de proporcionar "apoyo financiero y psicológico" de manera individualizada, esto es, una vez analizadas todas las circunstancias derivadas de la presentación de la comunicación. Un sistema que se basa en el modelo francés y que tiende a alejarse de los populares programas de protección al *whistleblower* de EE.UU. basados en toda una serie de incentivos y medidas económicas y financieras de distinta índole.

Con todo, en lo concerniente a la norma española, su efectividad no está, en modo alguno, garantizada, sino que estará supeditada al número de personas que decidan informar sobre alguna de las acciones u omisiones a que se refiere el artículo 2 de ley. En cualquier caso, prevemos un incremento exponencial del número de informantes en los próximos años, por lo que convendrá prestar atención detenida al momento de creación de esta autoridad para ver si es capaz de otorgar ayuda individualizada a un colectivo que se verá, frecuentemente, en clara situación de vulnerabilidad.

Con todo, el ámbito personal de la ley dispone de un alcance manifiestamente más restrictivo con respecto al material puesto que, pese a que protege a los sujetos informantes con independencia del canal de información empleado,[44] no incluye a categorías que, en determinadas situaciones, requerirían de protección, como podría ser el personal directivo o los miembros de los órganos de gobierno. También deja a su suerte a las organizaciones que asisten o realizan actividades de apoyo o investigación junto a la persona informante, entre las que se incluyen asociaciones

[43] Esta se menciona tímidamente en el preámbulo de la misma como "la expresión de su comportamiento cívico y se contrapone a otras actuaciones que, por el contrario, resulta indispensable excluir de la protección, tales como la remisión de informaciones falsas o tergiversadas, así como aquellas que se han obtenido de manera ilícita".

[44] Un avance considerable puesto que, el art. 28 del proyecto de ley, supeditaba la protección contra represalias al seguimiento de un sistema de canales de denuncia a tres niveles en el que la comunicación, en primer término, debía realizarse por canales internos y externo. Una exigencia que se basaba en la "preferencia" de que la información sobre prácticas irregulares debía conocerse, en primer término, por la propia organización en aras de que estas fueran corregidas o reparadas "lo antes posible los daños". Un criterio restrictivo y no previsto expresamente por la Directiva que, finalmente, fue eliminado en las enmiendas del Senado.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

de protección a las personas informantes u organizaciones no gubernamentales (ONG), entre otras.

Ni que decir tiene que se trata de una de las grandes diferencias con otras legislaciones de nuestro entorno, como la ley francesa anteriormente citada que, en el art. 2.1º, abarca dentro de la protección a los "facilitadores", entendiéndose como tal "toda persona física o toda persona jurídica de derecho privado sin ánimo de lucro que ayude a un denunciante a realizar una denuncia o denuncia (…)". Una definición que deja cabida a las ONG o asociaciones en una firme apuesta, entendemos, por otorgar protección a aquellas organizaciones que han estado estrechamente ligadas a los informantes. Es más, sigue la senda de los fructíferos resultados cosechados a lo largo de las pasadas décadas en EE.UU., donde este tipo de organizaciones han incentivado la denuncia de irregularidades hasta el punto de consolidar un marco jurídico de protección efectiva de los derechos e intereses de este colectivo en clara situación de vulnerabilidad.[45]

4.- Reflexiones conclusivas

Es indudable que la función de las personas informantes no puede circunscribirse a su mera catalogación como meros "denunciantes", sino que su papel se reconceptualiza como un verdadero defensor de la legalidad y del interés público.

[45] En EE.UU, las ONG disponen de una amplia experiencia en la protección del denunciante, desarrollando un papel clave en su protección. Entre las más destacadas, *Empower Oversight Whistleblowers & Research* (EMPOWR) trabaja para ayudar a las personas con información privilegiada a documentar y denunciar la corrupción a las autoridades correspondientes, al mismo tiempo que busca que las autoridades rindan cuentas para actuar sobre esos informes (https://empowr.us/). El *Proyecto de Responsabilidad Gubernamental* (GAP) es un grupo de interés público no partidista que promueve la responsabilidad gubernamental y corporativa al proporcionar representación legal a los denunciantes, proporcionando asesoramiento y apoyo legal y estratégico a empleados que pretenden denunciar o han denunciado una conducta indebida. GAP también lidera campañas para promulgar leyes de protección de denunciantes tanto a nivel nacional como internacional (https://www.whistleblower.org). Por su parte, *Consejeros de Seguridad Nacional* (NSC), son un bufete de abogados de interés público sin fines de lucro que están especializados en denuncia de irregularidades en ámbito laboral (http://www.nationalsecuritylaw.org). El *Centro Nacional de Denuncias* (NWC) ayuda a los denunciantes a que encuentren abogados que los representen, abogando por políticas que protejan y recompensen a los denunciantes (https://www.whistleblowers.org) o el *Proyecto sobre Supervisión Gubernamental* (POGO), una organización de control independiente que trabaja estrechamente con denunciantes del gobierno y promueve reformas mediante la denuncia de casos de corrupción y los conflictos de intereses (http://pogo.org). *Contribuyentes Contra el Fraude* promueve la efectividad de la Ley de Reclamos Falsos y los programas federales de denunciantes (https://taf.org) o *The Signals Network* (TSN), que apoya a los denunciantes que han compartido información de interés público con la prensa sobre mala conducta empresarial o abusos de los derechos humanos (thesignalsnetwork.org). Finalmente, destaca Denunciantes de América (WoA), que se centran en ayudar a los denunciantes que han sufrido represalias (https://whistleblowersofamerica.org)

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

Y lo cierto es que la reciente aprobación de la Ley 2/2023, pese a avanzar notablemente en la creación de un marco jurídico integral de protección al informante, se queda a medio camino en la adopción de una legislación garantista de la protección del informante.

Buena muestra de ello se aprecia en la existencia de ciertas dudas sobre si esta alcanza o no el nivel de protección requerido por la Directiva 2019/1937, teniendo en consideración que esta ha cumplido con un trámite parlamentario mínimo en cuanto a la técnica diferida de transposición. En particular, debe apuntarse la falta de coherencia de esta ley con normas del resto del ordenamiento jurídico nacional, cuestión que viene motivada por deficiencias sistémicas que parten desde un cierto grado de confusión a lo largo de la citada ley en la denominación de la figura del informante hasta otros preceptos, como los relativos a la designación del DPD, en los que se evidencia una técnica legislativa imprecisa.

Ya adentrándonos en el ámbito de aplicación de esta ley, desde una perspectiva objetiva, esta se centra en la denuncia de tales infracciones a través de canales internos y externos de información. Sin embargo, nada establece acerca de otras conductas como podría ser el incumplimiento de las políticas internas o códigos éticos que las organizaciones llevan implementando en los últimos años y décadas, así como otras conductas relacionadas con el abuso de poder que se producen en el seno de estas. Asimismo, esta ley no exime de responsabilidad penal a las personas que informen de casos de corrupción, un déficit considerable que conllevará la desprotección de potenciales informantes que ayudarían a destapar casos de perjuicios de primer orden para el interés público. A modo de *lege ferenda*, una ulterior reforma de la ley española debería pivotarse sobre la supresión de la responsabilidad penal del informante, sin perjuicio de aquellos delitos penales que resulten independientes de la acción de informar o denunciar como las amenazas o daños a la seguridad personal que no estén relacionados con la elaboración de un informe o la divulgación de información conforme a la citada ley.

Por su parte, es perceptible un ámbito de aplicación subjetivo de esta ley sumamente restrictivo, pues deja fuera de esta ley al personal directivo o los miembros de los órganos de gobierno que podrían actuar a modo de potenciales informantes con información relevante que podría amenazar el interés público. Tampoco entran dentro del ámbito de protección las organizaciones que asisten o realizan actividades de apoyo o investigación junto a la persona informante, como podrían ser las asociaciones que actúan en defensa de las personas informantes u ONG, entre otras. Consecuentemente, deberá realizarse una interpretación extensiva del ámbito subjetivo de la Ley 2/2023 del que deriva *prima facie* del tenor literal a fin de comprender a un amplio elenco de personas físicas y jurídicas –incluyendo, en el caso de esta última, a toda aquella organización que apoye, asista o investigue

Sección Estudios y Artículos
Los retos de la protección de las personas informantes en España tras la aprobación de la Ley 2/2023
por Jorge Viguri Cordero
Págs. 271-298
DOI: https://doi.org/10.51915/ret.313

la acción de informar junto al informante que actúa como interesado en el procedimiento–.

Finalmente, debe advertirse de que la Ley 2/2023 confiere a la futura AIPI la posibilidad de proporcionar "apoyo financiero y psicológico" a los informantes. Sin bien, puede predecirse que este tipo de ayudas se articularán de manera excepcional por lo que, sin perjuicio de ulterior desarrollo reglamentario que especifique las condiciones requeridas para suministrar apoyo financiero al informante, para que las personas puedan acceder a dicha protección deberá existir un fuerte compromiso por parte de esta autoridad independiente. Esto deberá incluir tanto una voluntad inequívoca de asistir a los informantes como recursos económicos suficientes para proveer efectivamente dichas ayudas.

Bibliografía

ALIAGA RODRÍGUEZ, R. 2022. "La denuncia anónima como instrumento de transparencia y protección de los denunciantes", *Revista Española de la Transparencia*, núm. 14: 57-78.

AMOEDO BARREIRO, D. 2017. "Elementos esenciales para un sistema de protección del informante", *Revista Internacional de Transparencia e Integridad,* núm. 4: 1-8.

AMOEDO BARREIRO, D. 2018. "Los sistemas informáticos de detección de malas prácticas, herramientas esenciales para la prevención de la corrupción". *Revista Internacional de Transparencia e Integridad*, núm. 6: 1-7.

BENÍTEZ PALMA, E. 2018. "El control externo y el *whistleblowing* (canales de denuncia)", *Revista Española de Control Externo*, vol. XX, núm. 59: 11-42.

BUENO SÁNCHEZ, J. M. 2022. "Oportunidad legal y necesidad democrática de crear una Autoridad Administrativa Independiente de Lucha contra la Corrupción y Protección del Denunciante", *Revista de administración pública*, núm. 217: 209-240.

CHEVARRÍA F., SILVESTRE M. 2013. *Sistemas de denuncias y de protección de denunciantes de corrupción en América Latina y Europa.* Colección Documentos de Trabajo. Serie Estados de la cuestión Área Institucionalidad Democrática, núm. 2:1-116. (http://sia.eurosocial-ii.eu/files/docs/1400663798-DT2.pdf).

CLEMENTE MARTÍNEZ, J. 2022. Los principios de buen gobierno de la nueva Ley Valenciana 1/2022. *Estudios de Deusto: revista de Derecho Público*, vol. 70. núm. 2: 115-152.

FERNÁNDEZ AJENJO, J. A. 2020. "Comentarios a la Directiva UE 2019/1937 relativa a la Protección de las personas que informen sobre infracciones del Derecho de la Unión", en RODRÍGUEZ GARCÍA N., y RODRÍGUEZ LÓPEZ F., (Dirs.), *Compliance y*

CC BY SA

Justicia Colaborativa en la prevención de la Corrupción, Valencia: Tirant lo Blanch: 111-139.

GARCÍA MAHAMUT R. 2023, "Graves anomalías en el primer proceso de selección de la presidencia y adjuntía de la AEPD al amparo de la LOPDGDD y del RGPD: algunas propuestas de reforma" en PAUNER CHULVI C., GARCÍA MAHAMUT R., TOMÁS MALLÉN B., (Eds.), *La implementación del Reglamento General de Protección de Datos en España y el impacto de sus cláusulas abiertas*, Valencia: Tirant lo Blanch, 179-199.

GARCÍA MORENO B. 2022. "La figura del whistleblower", en: JORDI GIMENO BEVIÁ J., LÓPEZ DONAIRE Mª B., (dirs.), *La directiva de protección de los denunciantes y su aplicación práctica al sector público,* Valencia, Tirant Lo Blanch: 29-52.

GARCÍA MORENO, B. 2020. *Del whistleblower al alertador. La regulación europea de los canales de denuncia*, Valencia, Tirant Lo Blanch: 1-342.

GARRIDO JUNCAL, A. 2019. "La protección del denunciante: regulación autonómica actual, novedades normativas y propuestas de futuro". *Revista de Estudios de la Administración Local y Autonómica. Nueva época*, núm. 12: 126-151.

LEO CASTELA J. I. 2021. *Gestión de riesgos legales y compliance corporativo,* Valencia. Tirant lo Blanch: 1-206.

MIRANZO DÍAZ J. 2019. "La nueva Directiva de protección del denunciante: un análisis desde el Derecho público", *Revista General de Derecho Europeo*, núm. 49: 361-385.

NAVARRO MEJÍA, I. 2021. "La falta de transposición de una directiva europea en materia reservada a ley orgánica. Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea de 25 de febrero de 2021. Asunto C-658/19", *Revista de las Cortes Generales,* núm. 111: 611-628.

PAUNER CHULVI C. 2023. "Protección de las personas informantes en la Directiva (UE) 2019/1937 y tratamiento de datos de carácter personal. Breve referencia a la Ley 2/2023 de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción", en PAUNER CHULVI C., GARCÍA MAHAMUT R., TOMÁS MALLÉN B., (Eds.), *La implementación del Reglamento General de Protección de Datos en España y el impacto de sus cláusulas abiertas*, Valencia: Tirant lo Blanch: 265-295.

PÉREZ MONGUIÓ J. M. 2020. "Whistleblower y las dificultades para su implantación en España e Italia", en: SÁNCHEZ DE DIEGO y FERNÁNDEZ DE LA RIVA M., Sierra-Rodríguez J. (Coords.), *Transparencia y participación para un gobierno abierto*. *El Consultor de los Ayuntamientos, La Ley:* 227-247.

CC BY SA

DOI: https://doi.org/10.51915/ret.313

PÉREZ TRIVIÑO, J. L. 2018. "Whistleblowing", *Eunomia. Revista en Cultura de la Legalidad*, núm. 14: 285-298.

RAGUÉS I VALLÉS, R. 2006. "¿Héroes o traidores? La protección de los informantes internos (wistleblowers) como estrategia político-criminal", *InDret,* núm. 3: 1-19.

RODRÍGUEZ-MEDEL NIETO, C. 2019. "La protección de los informantes –*whistleblowers*– y las garantías de los investigados. Análisis de la propuesta de Directiva de la Unión Europea y en España de la proposición de ley integral de lucha contra la corrupción y protección de los denunciantes", *Revista de Estudios Europeos*, núm. extraordinario monográfico 1/2019: 225-245.

SIERRA RODRÍGUEZ, J. 2020, "Impulso europeo al whistleblowing y las autoridades de integridad". *Eunomía. Revista en Cultura de la Legalidad*, núm. 19: 64-85.

SIERRA RODRÍGUEZ, J. 2020. "Anonimato y apertura de los canales de denuncia de la corrupción". *Revista General de Derecho Administrativo*, núm. 55: 1-41.

SIERRA RODRÍGUEZ J. 2022. "La autoridad independiente de protección del informante en la ley 2/20231". *Revista Española de Control Externo*, vol. XXIV, n.º 72: 78-103.

STRACK, G. 2011. "Whistleblowing in Germany", en: ARSZUŁOWICZ M., GASPARSKI W. (Eds.), *Whistleblowing: In defense of proper action*, New Brunswick, New Jersey: 109–124.

VESTRI, G. 2019. "Aproximación al sistema de «whistleblowing». Un nuevo desafío para la Administración pública española". *Revista General de Derecho Administrativo*, núm. 51.

VILLORIA MENDIETA, M. 2021. "Un análisis de la Directiva (UE) 2019/1937 desde la ética pública y los retos de la implementación", *Revista Española de la Transparencia*, núm. 12: 15-24.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local

Jaime Clemente Martínez[1]

Universitat Jaume I de Castelló

España

ORCID: 0000-0002-3092-0401

RECIBIDO : 28/04/2023
ACEPTADO : 7/07/2023

Este trabajo ha sido realizado en el marco del proyecto del Ministerio de Ciencia e Innovación DATATRANSCO con referencia n.º PID2021-128309NB-I00.

RESUMEN: Ante el auge de casos de corrupción en las administraciones, en especial en las locales, cada vez resulta más conveniente la utilización de técnicas avanzadas para evitarlos. El uso de las bases de datos a las que tienen acceso las entidades locales y las técnicas de *data mining* supone una nueva oportunidad para que los consistorios puedan evitar fraudes en sus expedientes. Por ello, en el presente artículo se aborda la gran utilidad de dichas bases de datos y de la minería de datos para detectar conflictos de intereses y corruptelas municipales que, de otra forma, pasarían desapercibidas. Asimismo, se hace un especial hincapié en el margen de actuación que la normativa de protección de datos otorga en este ámbito y qué retos deben abordarse para conseguir exprimir el potencial de dichas bases de datos con fines antifraude para poder luchar adecuadamente contra la lacra de la corrupción local.

1 Profesor de Derecho Constitucional de la Universitat Jaume I (acreditado como Profesor Contratado Doctor). Ha ejercido como funcionario de carrera de administración local con habilitación de carácter nacional, subescala de Secretaría-Intervención. Asimismo, también ha desempeñado el cargo de Subdirector General en la Conselleria de Transparencia de la Generalitat Valenciana y el puesto de responsable del Área de Administración Local en la Subdelegación del Gobierno en Castellón.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

PALABRAS CLAVE: Bases de datos, *data mining*, prevención de la corrupción, administración local, conflictos de intereses.

CONTENIDOS: 1.-Introducción. 2.-La oportunidad de uso de bases de datos con fines anticorrupción por la administración local. 3.-El *data mining* como instrumento de prevención de conflictos de intereses en entidades locales: el caso de MINERVA 4.-Dificultades y retos en materia de protección de datos para emplear las bases de datos y el *data mining* como herramienta antifraude. 5.-Conclusiones. -Bibliografía.

Databases and *data mining* as anti-corruption tools in local administration

ABSTRACT: With the rise in corruption cases within administrations, particularly in local councils, there is an escalating need to employ advanced techniques as a means to prevent such unlawful behaviors. The use of databases to which local entities have access and data mining techniques provide a new opportunity for the councils to prevent fraud. Hence, this article

addresses the significant value of databases and data mining in detecting conflicts of interest and municipal corruption that would, otherwise, remain undetected. Furthermore, special emphasis is placed on the scope of action that data protection regulations offer in this area as well as the challenges that need to be addressed in order to harness the power of these databases for anti-fraud purposes. Consequently, this study aims at tackling the scourge of local corruption appropriately.

KEYWORDS: Databases, *data mining*, prevent corruption, local administration, conflict of interest.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

1.- Introducción

Las administraciones locales, para poder efectuar adecuadamente las competencias que tienen atribuidas deben operar con una serie de bases de datos, tanto propias del consistorio como otras externas, para poder ejecutar las políticas públicas y resolver los expedientes administrativos a su cargo. A pesar de la habitual utilización de dichas bases por los ayuntamientos, en la práctica, las mismas no se vienen utilizando frecuentemente para localizar fraudes en expedientes administrativos[2].

Ello supone una gran oportunidad para las entidades locales, que pueden aprovechar las bases de datos a su disposición para detectar conflictos de interés y en su caso posibles corruptelas que, de otra forma, habrían pasado desapercibidas. A lo que debe sumarse la utilización del *data mining* de MINERVA como herramienta de prospección de datos en la gestión de fondos europeos, que ha supuesto un punto de partida inédito para prevenir el fraude. Téngase en cuenta que, actualmente, los casos de corrupción siguen siendo elevados[3], y la utilización de todo tipo de medidas para prevenirlos resulta altamente conveniente, por lo que dichas bases de datos y la minería de datos proporcionan una opción para conseguir la aplicación efectiva de los principios de imparcialidad y ausencia de conflicto de intereses, entre otros previstos en el artículo 26 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno y, en general, conseguir la consecución del interés general constitucionalmente previsto en el artículo 103 de la Constitución española.

Si bien, la utilización de las bases de datos y de la minería de datos con fines anticorrupción encuentran como límite en su utilización la protección de datos personales y la ausencia de una exigencia legal de que tengan que realizarse. Por ello, mediante el presente trabajo se presente analizarse con detalle el alcance y

[2] En este sentido, CAMPOS ACUÑA (2021), indica como el *data mining*, que permite buscar de forma masiva en bases de datos con fines anticorrupción (como posteriormente se indicará) se implanta en la gestión de fondos europeos, incluidos los que gestionan entidades locales, ya que: "los requerimientos exigidos en la lucha contra el fraude y la corrupción no se contemplan con el alcance requerido en la dinámica de gestión tradicional". Lo que demuestra que actualmente no se vienen utilizando frecuentemente las bases de datos ni por supuesto el *data mining* con fines anticorrupción en los ayuntamientos, ya que sino seguramente no hubieran sido necesarias dichas medidas implantas por la Comisión Europea para ejecutar sus fondos.

[3] A este respecto, puede consultarse el repositorio de datos por procesos de corrupción del Consejo General del Poder Judicial donde se puede atestiguar la cantidad de procesos de corrupción que existen, ya que de hecho a fecha del cuarto trimestre del 2022 existen en España un total de 41 condenados por delitos relacionados con la corrupción.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

potencial de estas herramientas que sirven, en efecto, para evitar fraudes en la administración local.

Para efectuar dicho estudio se aborda, primero como las entidades locales podrían hacer uso de las bases de datos a su alcance para evitar fraudes, seguidamente se expone como los ayuntamientos puedes utilizar el *data mining* y en especial la herramienta MINERVA para prevenir la corrupción y finalmente se exponen los principales límites a su utilización y cambios legales que serían necesarios para permitir un uso completamente y así prevenir corruptelas fácilmente en las entidades locales. Con todo ello se pretende poner en foco en las grandes posibilidades que tienen dichas entidades de usar las bases de datos y el *data mining* para conseguir una administración más íntegra y cómo sería preciso un importante apoyo del Estado en realizar reformas normativas para permitir un uso completo de dichas bases en beneficio de conseguir el interés general de la ciudadanía.

2.- La oportunidad de uso de bases de datos con fines anticorrupción por la administración local

Como punto de partida, conviene identificar qué bases de datos pueden utilizar los consistorios locales para detectar fraudes y por ello, la primera que pueden utilizar las entidades locales es el registro de entrada y de salida. Un registro que las administraciones utilizan para reflejar aquellas personas físicas o jurídicas que ha interactuado con ella presentando o recibiendo documentos. La utilización de dichos datos se suele utilizar principalmente a efectos de envío de comunicaciones a interesados sobre expedientes, si bien ello no impide que la utilización de dicha información se efectúe también con fines preventivos de corrupción. Tengamos en cuenta que los registros de entrada y de salida de dichas entidades contienen información sobre las direcciones postales y direcciones electrónicas de los interesados, que pueden resultar una técnica de prevención de la corrupción.

A modo de ejemplo, podríamos utilizar dicha base de datos para verificar si la dirección postal de un contratista coincide con la de un responsable político que le ha adjudicado el contrato, y es que, si fuera así, posiblemente tengan una relación personal o familiar que no hayan indicado, lo que, en consecuencia, supondría un eventual conflicto de interés. De este modo, en el presente ejemplo las bases de datos servirían para prevenir una posible situación de corrupción que podría producirse al adjudicar un responsable político un contrato a alguien con quien mantiene una determinada relación. Ello supondría un supuesto en el que el órgano de contratación debería haberse abstenido, conforme establece el artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), algo que debe vigilarse especialmente en los ayuntamientos ya que, como apunta Campos Acuña (2015:79), las situaciones en las que puede generarse una situación

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

de abstención son más frecuentes en los ayuntamientos que en otras administraciones.

Otro ejemplo donde podrían utilizarse la base de datos del registro de entrada y salida para prevenir un fraude es en referencia a la comprobación del dominio de las direcciones de correo electrónico. Los interesados informan habitualmente de una dirección de correo electrónico a la que quiere que se le avise de la puesta disposición en sede de una notificación electrónica, conforme prevé el art. 41.1.b *in fine* de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[4] (LPACAP). En este caso, de nuevo podría verificarse si el dominio de la dirección de correo electrónico de un contratista al que se le ha adjudicado un contrato coincide con el dominio del correo electrónico personal del concejal al que se la ha adjudicado ese contrato. De ser así, es posible que haya sido empleado de dicha empresa contratada, por lo que debería haberse abstenido a la hora de efectuar dicha adjudicación. Tengamos en cuenta que, habitualmente, los operadores jurídicos del ayuntamiento conocen la empresa para la que trabaja un concejal, en la medida en que las administraciones locales suelen ser pequeñas y el número de concejales no es muy elevado.

Si bien, podría darse la situación en que un cargo electo esté trabajando para una empresa y ello sea totalmente desconocido para el personal del ayuntamiento, en tanto en cuanto si dicho concejal no tiene asignada una dedicación exclusiva o parcial[5], es posible que la entidad local no sea conocedora del nuevo puesto de trabajo que desempeña. Todo ello, sin perjuicio de la declaración de actividades que debe presentar cuando toma posesión como concejal y que debe actualizar cuando se produzcan cambios, conforme prevé el art. 30.2.b del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Local (ROF)[6], pero quizás dicho concejal no actualizó a tiempo dicha declaración[7] por lo que podría haberse ignorado por la entidad local el cambio de empleo del cargo electo. Lamentablemente, como

[4] Dicho art. 41.1.b *in fine* LPACAP establece: "Adicionalmente, el interesado podrá identificar un dispositivo electrónico y/o una dirección de correo electrónico que servirán para el envío de los avisos regulados en este artículo, pero no para la práctica de notificaciones".

[5] El art. 75 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LRBRL) establece los regímenes de dedicación exclusiva y parcial al que tienen acceso los cargos electos locales.

[6] Dicho art. 30.2.b ROF establece que debe actualizarse dicha declaración de intereses: "Cuando se produzcan variaciones a lo largo del mandato. En este caso el término para comunicar las variaciones será de un mes a contar desde el día en que se hayan producido".

7 A pesar de ser una exigencia legal, no son pocos los ejemplos en los que se observa que los cargos electos locales no han actualizado a tiempo las declaraciones de intereses (con información sobre bienes, actividades, etc. de los concejales) que prevé el art. 31 ROF.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

apunta Arnaldo Alcubilla (2009:535), la obligación de presentación, y también de actualización, de una declaración de intereses puede ser fácilmente omitida por un cargo local, ya que no comporta sanciones.

Con todo, en los dos ejemplos indicados, las bases de datos del registro de entrada y de salida del ayuntamiento nos proporcionan información valiosa sobre posibles conflictos de intereses que puedan ocasionarse y que de detectarse situaciones como las indicadas, u otras que generan conflictos, podría realizarse una recusación (prevista en el art. 24 LRSJP) hacia los cargos públicos que deberían haberse abstenido.

Así pues, el citado registro de intereses se trata de la siguiente base de datos que se podría utilizar para obtener información valiosa para prevenir la corrupción en la administración local. Este registro de intereses se trata de un registro municipal que, conforme el artículo 75.7 LRBRL, incluye información sobre los bienes patrimoniales y liquidaciones de impuestos estatales y declaraciones sobre actividades desarrolladas que puedan generarle ingresos al concejal. De tal modo, dichos datos pueden utilizarse para prevenir eventuales conflictos de intereses o situaciones en las que se pueda caer en el fraude. Partiendo de la información del registro de actividades, ello nos proporciona información sobre el lugar de trabajo que genera ingresos a dicho concejal, en consecuencia, puede advertirse con facilidad aquellas situaciones en las que dicho cargo electo debería abstenerse a la hora conceder un contrato administrativo o una subvención, si el posible beneficiario es dicha empresa o entidad que le genera ingresos.

Téngase en consideración que el hecho de que un cargo público trabaje en una empresa no es impedimento para que la misma no pueda participar en ningún proceso de adjudicación de contratos, concesiones o subvenciones que efectué el ayuntamiento del citado concejal, simplemente lo que deberá producirse es la abstención de dicho concejal en el procedimiento y la asunción temporal por otro cargo electo de las funciones del edil, que deberá abstenerse al tener una relación de servicio con la empresa conforme prevé el art. 23.2.e LRJSP[8].

Si bien, la problemática también reside en el hecho en que dicho registro de actividades no disponga de un histórico de los diferentes puestos de trabajo que ha desempeñado el concejal, ya que el art. 75.7.a LRBRL establece que solo debe hacerse constar en dicho registro: "actividades que proporcionen o puedan proporcionar ingresos económicos", con lo cual la posibilidad de controlar la obligatoriedad de abstención de un cargo electo se ve limitada a las entidades por

[8] Dicho art. 23.2.e LRJSP establece: "Tener relación de servicio con persona natural o jurídica interesada directamente en el asunto, o haberle prestado en los dos últimos años servicios profesionales de cualquier tipo y en cualquier circunstancia o lugar".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

las que actualmente el concejal percibe ingresos o está previsto que le generen ingresos durante el mandato público. En consecuencia, si el cargo electo ha desempeñado en los dos últimos años, un puesto de trabajo en la entidad que eventualmente pueda tener una relación con el área del ayuntamiento del que es competente el concejal, ello no podrá detectarse a través del registro de intereses y conforme al citado art. 23.2.e LRJSP también sería una causa de abstención, ya que se generaría una eventual confusión entre intereses públicos y privados, que como apunta Fibla Nicolau (2010:182) debe evitarse mediante la abstención para evitar "situaciones comprometidas y sospechosas". Por otra parte, a la vista de esa entremezcla de interés públicos y privados, téngase presente que el ejercicio de esas facultades de control por la entidad local no solamente es coherente con las obligaciones positivas que se desenvuelven en las relaciones verticales entre la propia administración y cargo electo afectado, sino que puede tener una proyección en lo que concierne a las relaciones horizontales entre la posición de dicho cargo electo y los derechos e intereses de otras personas afectadas, así lo ha estudiado recientemente TOMÁS MALLÉN (2022).

La declaración de bienes patrimoniales y participación en sociedades, prevista en el art. 75.7 párrafo segundo LRBRL, es también una fuente de información en la que podrían haber situaciones que pudieran generar un eventual fraude en la administración con el fin de evitarlas. Por un lado, podríamos encontrar información referente a las participaciones de un concejal en una empresa, lo que evidentemente le generaría una situación en la que, de nuevo, procedería una causa de abstención. Por otro lado, encontraríamos la información sobre las propiedades inmobiliarias del concejal, para detectar posibles bienes a nombre del mismo que pueden verse afectados por determinadas decisiones urbanísticas que pueda tomar o en las que pueda participar dicho cargo electo.

Si bien, en este último supuesto de los bienes inmuebles del cargo electo resultaría más complejo poder descubrir un fraude a través de dicha información, ya que cuando se proporciona información sobre el patrimonio inmobiliario no siempre se incluye la localización exacta de la propiedad. Ello se produciría, en primer lugar, si el inmueble está inscrito en el Registro de la Propiedad posee un número de inscripción registral que, de constar, debe ser indicado en dicha declaración de intereses conforme el art. 31.1.a ROF. Ahora bien, tengamos en consideración que la inscripción en el Registro de la Propiedad es voluntaria y, por tanto, ante la falta de inscripción registral en el mismo el cargo electo no incluiría dicha referencia, dificultando, *a priori*, la ubicación concreta del inmueble.

En todo caso, teniendo en cuenta que el citado art. 31.1.a ROF establece que debe poderse identificar los inmuebles, lo que sin duda se cumpliría al establecer la localización exacta, pero en la práctica encontramos múltiples declaraciones

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

aprobadas por plenos[9] de entidades que parecen haber establecido referencias más genéricas para la identificación de los inmuebles o bien, que estableciendo referencias para identificar exactamente dónde está el bien, los cargos electos han preferido dar una referencia no tan precisa de la ubicación del inmueble[10].

Ante estas situaciones de falta de precisión de la ubicación de los inmuebles, resulta más complejo utilizar los datos para prevenir fraudes. Aun así, si existe el compromiso del ayuntamiento de utilizar dichos datos para lograr un buen gobierno podría aprovecharse también, por ejemplo, la referencia a una partida en la que se encuentra un terreno de un concejal para que, si el mismo adopta una decisión urbanística que afecta a dicha zona del municipio, se le emplace para que demuestre que no adopta la decisión para beneficiar un terreno de su propiedad o que se abstenga de tomar la decisión.

La siguiente base de datos a disposición de la entidad local de la que se puede obtener información para prevenir conflictos de intereses es el registro de personal del propio ayuntamiento. En este caso, la información de dicho registro sirve para evitar posibles actuaciones fraudulentas en las que puede incurrir, principalmente, los funcionarios y el personal laboral de la entidad local a la hora de tramitar determinados expedientes. En estos casos, sucede de forma semejante como ocurría con los casos de concejales indicados, se pueden cotejar los datos postales

[9] Sobre cómo deben configurar dichas declaraciones de bienes los Plenos de las entidades locales véase: MARÍN PÉREZ (2007).

[10] Encontramos ejemplos variados en este sentido, por un lado entidades locales que directamente solo han establecido en el modelo de declaración que se indique la ciudad donde se ubican los inmuebles, de manera que resulta imposible identificar la zona aproximada del municipio donde se encuentra, ello lo encontramos en las declaraciones del Ayuntamiento de Parla (pueden verse dichas declaraciones de bienes en el portal de transparencia de la entidad local aquí: https://transparencia.ayuntamientoparla.es/transparencia-municipal/organigrama-del-ayuntamiento/, consultado el 26/02/2023). Por otro lado, otras entidades locales establecen que debe indicarse el emplazamiento de los inmuebles, como es el caso del Ayuntamiento de Tineo (puede verse aquí: https://www.tineo.es/declaracion-de-bienes-y-actividades, consultado el 27/02/2023) y aunque ello ha hecho que algunos concejales identifiquen la calle y ubicación exacta otros han establecido simplemente el barrio, la partida o directamente solo el municipio donde se encuentra, dificultando así la posibilidad de usar dichos datos para prevenir fraudes en la administración local como planteamos. Algunos ayuntamientos han establecido modelos donde indican que debe identificarse el lugar del inmueble, lo que *a priori*, parece una referencia suficiente para que se indique la ubicación precisa del mismo, como es el caso del Ayuntamiento de Sariegos (puede verse aquí: https://www.sariegos.es/ayuntamiento/transparencia/declaracion-bienes, consultado el 28/02/2023) aunque curiosamente al establecer un espacio tan pequeño en la cuadrícula para introducir el dato del lugar del inmueble la mayoría de concejales han optado por indicar solo el municipio donde está la propiedad, circunstancia que impide de nuevo obtener información precisa, lo que de nuevo no permite aprovechar la eventual información que podría obtenerse de dicho registro de intereses para fines anticorrupción en ayuntamientos.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

de los empleados municipales que tramiten un determinado expediente para poder hallar, en su caso, posibles situaciones en las que quizás deberían haberse abstenido. Ello podría suceder, por ejemplo, por coincidir su domicilio con el de un posible contratista o beneficiario de una ayuda pública, situación que, como se ha expuesto en los citados casos de concejales, podría generar un eventual conflicto de interés. Así pues, en caso de dicho cotejo debería darse a los interesados la oportunidad de alegar sobre si no procede dicho conflicto de interés antes de decidir sobre si en efecto procediese recusarle sobre un expediente.

Puede utilizarse también otra herramienta para controlar posibles fraudes en la administración a través de la Base de Datos Nacional de Subvenciones (BDNS), regulada en el Real Decreto 130/2019, de 8 de marzo, que es un registro integrado de aquellas ayudas que se han concedido por las diferentes administraciones públicas. Puede resultar de gran interés dicha base de datos como herramienta para prevenir los fraudes en la medida en que, como requisito habitual para conseguir una subvención por parte del ayuntamiento, no se debe haber recibido otra subvención por el mismo concepto concedida por otra administración, ya que como apunta Fernández Ajenjo (2019:194), dicha BDNS permite una colaboración interadministrativa para "mejorar la eficacia y evitar solapamientos en las subvenciones públicas".

Para tratar de evitar esto, actualmente las administraciones concedentes acostumbran a solicitar una declaración responsable al interesado para que el mismo informe de que no ha recibido otra ayuda pública por el mismo concepto[11], si bien, cabe la posibilidad de que los interesados falseen dicha declaración. Por tanto, con el fin de comprobar la veracidad de dichas declaraciones puede utilizarse la BDNS, que permite comprobar las subvenciones recibidas por los interesados y, por tanto, el ayuntamiento puede evitar conceder ayudas que ya han sido subvencionadas por otra administración, lo que supondría un fraude para el erario público. En este sentido, Molina Mesa (2015:315) destaca como, en efecto, dicha base de datos ayuda notoriamente a la labor de fiscalización que realizan tanto los órganos de control interno de las entidades locales como el control externo que efectúa el Tribunal de Cuentas, ya que permite obtener información sobre ayudas públicas de forma agrupada.

El Registro Oficial de Licitadores y Empresas Clasificadas del Estado (ROLECE), supone el siguiente ejemplo de base de datos susceptible de utilización por las

11 En este sentido pueden consultarse diferentes modelos de declaración responsable establecidos por entidades locales que obligan al interesado a indicar que no ha recibido otra ayuda pública por el mismo concepto, para evitar duplicidad de ayudas. Véase, por ejemplo, las del Ayuntamiento de Murcia (http://www.murcia.es) o del Ayuntamiento de Boadilla del Monte (https://ayuntamientoboadilladelmonte.org).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

entidades locales para prevenir actividades corruptas. Este registro, recogido en el art. 337 LCSP, tiene como objetivo que las entidades puedan verificar la capacidad para contratar, la solvencia de la entidad entre otros aspectos[12]. En este sentido, y a efectos de evitar fraudes, consideramos especialmente importante que en dicho registro se inscriban también las prohibiciones para contratar que una determinada empresa pueda tener con una administración, de las previstas en el art. 71 LCSP. Si fruto de una actuación incorrecta de una empresa con la administración esta le declara una prohibición para contratar, si el resto de las administraciones públicas no son suficientemente conocedoras de dicha prohibición, podrán incurrir en el error de contratar de nuevo a dicha empresa. Así pues, el ROLECE debe servir como herramienta para localizar posibles prohibiciones para contratar que tenga una empresa, de forma que antes de adjudicar o formalizar un contrato el órgano de contratación debería entrar en dicho registro para verificar que no hay ninguna prohibición inscrita[13].

En efecto, dicho registro sirve como herramienta de prevención de la corrupción en la medida en que supone la forma más efectiva de que una administración pueda conocer la prohibición para contratar que han declarado otras. La problemática reside en si las administraciones y entes verdaderamente registran las prohibiciones para contratar que declaran ante dicho ROLECE, una cuestión que también se plantea Blanco López (2022) y ante la que tenemos difícil respuesta dada la ausencia de datos facilitados al respecto sobre el grado de cumplimiento de dicha exigencia por la Junta Consultiva de Contratación Pública del Estado y porque depende de la voluntad de cumplimiento de las administraciones de obligación de comunicar las prohibiciones que prevé el art. 338 LCSP. Si bien, el interrogante principal es si las administraciones antes de adjudicar consultan en dicho registro para observar posibles prohibiciones existentes, que supone una exigencia legal solo para los

12 El art. 96.1 LCSP establece que el ROLECE permite a las empresas inscritas acreditar frente a otras administraciones las: "condiciones de aptitud del empresario en cuanto a su personalidad y capacidad de obrar, representación, habilitación profesional o empresarial, solvencia económica y financiera y técnica o profesional, clasificación y demás circunstancias inscritas, así como la concurrencia o no concurrencia de las prohibiciones de contratar que deban constar en el mismo".

13 En este sentido puede resultar de interés una resolución de no formalización de un contrato a una empresa al que ya se le había adjudicado debido a que, con posterioridad a la adjudicación, pero antes de la formalización, el órgano de contrato de contratación consultó en el ROLECE la situación de la mercantil y se detectó que estaba incursa en una prohibición para contratar y fruto de ello no se formalizó. Esto supone un ejemplo de cómo se utilizó el ROLECE para detectar un fraude que trató de realizar la empresa, al no informar de sus prohibiciones para contratar, por lo que, si no hubiera sido por dicha base de datos, no se había descubierto dicha prohibición por el órgano de contratación y se le habría formalizado indebidamente dicho contrato. Puede consultarse la citada resolución de no formalización, referida al expediente nº201900000221 del Instituto Español de Oceanografía en la web https://contrataciondelestado.es/

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

procedimientos abiertos simplificados según art. 159.4.f.3.º LCSP, por lo que, en el resto de procedimientos, una ausencia de interés del órgano de contratación por querer evitar dichas prohibiciones consultando el ROLECE podría hacer que se incurran en fraudes en esta materia[14].

La siguiente base de datos que las entidades locales pueden utilizar como mecanismo para prevención del fraude es el Registro de la Propiedad. Como es conocido, permite acceder a datos tales como la identidad del propietario de una determinada vivienda y ello se pueden utilizar por una entidad local para verificar la auténtica propiedad de un vecino que, por ejemplo, va a suscribir un convenio con el ayuntamiento en el que pueda, por ejemplo, cederle dicho terreno para uso municipal[15].

Otra base de datos a la que se puede acceder fácilmente para consultar información y evitar posibles fraudes es el Registro Mercantil. En este caso, la información de esta base de datos puede ser relativa a quién es el administrador de una determinada empresa o qué volumen de negocio tiene y ello puede resultar de especial interés, por ejemplo, en materia de contratación administrativa[16]. Dichos datos del Registro resultan de interés en referencia a la solvencia económica en la gran mayoría de

[14] En esta materia de contratación pública destaca la reciente comunicación de la Comisión Europea que ha propuesto la creación de un Espacio de Datos sobre Contratación Pública, con el objeto, entre otros, de evitar la corrupción detectando patrones sospechosos junto con el uso de técnicas de inteligencia artificial. Cuando se produzca el desarrollo de dicho Espacio ello supondrá una nueva base de datos sobre la que realizar una adecuada investigación antes de cada licitación pública para así detectar posibles conflictos de intereses que hayan podido pasar desapercibidos. Al respecto véase: Comunicación de la Comisión sobre *Contratación pública: Un espacio de datos para mejorar el gasto público, impulsar la elaboración de políticas basadas en datos y mejorar el acceso de las pymes a las licitaciones* (2023/C 98 I/01).

[15] El uso de la información del Registro de la Propiedad por las administraciones locales viene siendo una circunstancia habitual para multitud de expedientes municipales, y en prueba de ello encontramos, por ejemplo, cesiones de terrenos privados a ayuntamientos para que los destinen a parking público de vehículos donde antes de firmar dicho convenio de cesión se

suele comprobar que el cedente del terreno es el verdadero propietario con copia de la inscripción registral. Sirva como ejemplo el convenio firmado por el Ayuntamiento de Ontinyent a este respecto (puede verse en https://www.ontinyent.es/), donde precisamente se observa cómo se ha consultado los datos del registro de la propiedad para verificar la propiedad de la parcela y así evitar posibles fraudes al evitar la entidad local suscribir un convenio de cesión de un terreno con alguien que verdaderamente no es su propietario.

[16] Si consultamos que datos pueden obtenerse con la nota informativa mercantil encontramos: capital social, representación social: administradores, cargos sociales y apoderados, nota informativa de inscripción, relación de cuentas depositadas, nota informativa de libros legalizados, asientos de presentación vigentes, situaciones especiales, posición de riegos de la sociedad, entre otros. Puede solicitarse dicha información de forma telemática en: https://sede.registradores.org/site/mercantil#/

CC BY SA

DOI: https://doi.org/10.51915/ret.314

procedimientos de contratación pública ya que conforme al artículo 87.3.a LCSP debe presentarse las cuentas anuales inscritas en el Registro Mercantil para acreditar dicha solvencia económica, con lo cual se viene realizando en la práctica la utilización de dicha base de datos para la comprobación de dicha solvencia y verificar que no existen fraudes al respecto.

Otro ámbito donde los datos de dicho Registro Mercantil resultan de interés es el relativo a los administradores de una empresa, en la medida en que, si un concejal o funcionario que interviene en un expediente es administrador de una empresa interesada en el mismo, dicho cargo público debería abstenerse del asunto conforme el citado art. 23 LRJSP. De tal modo, si se descubre con los datos del Registro Mercantil, por ejemplo, un conflicto por ser administrador de una empresa un concejal, que es órgano de contratación en un expediente en el que participa dicha mercantil, en estos casos, como apunta Galindo Caldés (2019:139), es mejor que se produzca la abstención antes que a la prohibición para contratar como medida para evitar fraudes locales y evitar también la nulidad del expediente de contratación.

De hecho, en el caso de que el administrador de una empresa sea un concejal, el mismo tendría que cumplir con la citada obligación del art. 30.2.b ROF de actualizar los datos de su registro de intereses, por lo que si no cumpliera con dicha exigencia (algo que hemos comentado que lamentablemente ocurre con frecuencia) el ayuntamiento podría detectarlo igualmente a través de los datos del Registro Mercantil. En consecuencia, la utilización de la base de datos de dicho Registro, en referencia a consulta de administradores de empresas, permitiría una doble labor, por un lado, vigilar que los concejales que sean administradores de entidades hayan actualizado dicha información en el registro de intereses y, por otro lado, hallar posibles conflictos de intereses cuando un concejal o funcionario sea administrador de una empresa que es interesada de un expediente municipal.

Como principal limitación de la información del Registro Mercantil que no puede ofrecerse a los ayuntamientos encontramos la lista de socios de una empresa. Dicha posibilidad no está entre los ítems que puede ofrecer el Registro Mercantil, y ello podría resultar de gran interés para advertir posibles conflictos de intereses en el caso de que alguno de los socios sea concejal o personal del ayuntamiento, en cuyo caso podría darse eventualmente prohibiciones para contratar, según prevé el artículo 71.1.g LCSP, que establece supuestos en los que determinados personas jurídicas no pueden contratar con una administración local cuando cargos electos, empleados de una administración o algunos de sus familiares tengan participación de dicha empresa.

La consulta de datos catastrales sirve también como referencia para cotejar posibles fraudes en la administración local. Como apunta Aragón Amunárriz (2020:23), la

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

colaboración entre el Catastro y las entidades locales aporta beneficios a ambas administraciones. Por ello, al ser los ayuntamientos colaboradores permanentes del Catastro pueden acceder a una serie de información contenida en dicha base de datos para utilizarla[17] para, por ejemplo, verificar adecuadamente el alta en el padrón del impuesto de bienes inmuebles[18]. Así pues, si se detecta una referencia catastral de un inmueble que no constaba en dicho padrón o que constaba con datos incompletos, puede realizarse una comprobación para verificar si, en efecto, dicho inmueble debería estar en el citado padrón con unos determinados datos y, en su caso, exigirle el pago de los recibos vencidos del impuesto de bienes inmuebles y, a partir de dicha fecha, darle de alta en el futuro.

Como apunta Puyal Sanz (2018:175), la información sobre el Catastro debe ser compartida a las diferentes administraciones interesadas, como los ayuntamientos que gestionan tributos ligados a inmuebles que constan en dicho registro, ya que ello permite mejorar la gestión de las políticas públicas. Si bien, todavía queda camino por recorrer para conseguir que dicho Catastro sea un instrumento totalmente eficaz para luchar contra la corrupción; por lo que aunque actualmente utilizamos el Catastro con frecuencia para evitar fraudes tributarios locales, lo cierto es que no debe dejarse de implementar medidas de mejora para que pase a ser un instrumento todavía mejor de lucha contra la corrupción en la administración local.

En definitiva, se han enumerado distintas bases de datos que pueden resultar de gran interés para las entidades locales a los efectos de detectar posibles fraudes. Evidentemente, no se trata de una lista de *numerus clausus*, por cuanto convergen otras bases de datos que permiten identificar potenciales corruptelas susceptibles de producirse en los ayuntamientos españoles. Las bases indicadas, así como los datos concretos que se encuentran las mismas resultan, a nuestro parecer, de suma

[17] Las entidades locales que sean Punto de Información Catastral pueden acceder a la siguiente información conforme al artículo segundo de la Resolución de 15 de enero de 2019, de la Dirección General del Catastro, por la que se aprueba el régimen de establecimiento y funcionamiento de los Puntos de Información Catastral que determina que se pueden consultar los siguientes aspectos que pueden resultar de interés para descubrir fraudes en las entidades locales: datos catastrales no protegidos, certificación de la referencia catastral y consulta de cartografía, consulta y certificación de datos catastrales protegidos, consulta y certificación de datos catastrales protegidos.

[18] Encontramos numerosos ejemplos que demuestran cómo las comprobaciones del Catastro han ayudado a las entidades locales a descubrir fraudes sobre el IBI. Aunque dichas actuaciones fraudulentas se han producido fruto de una valoración colectiva realizada por el Catastro también podrían descubrirse fraudes si es el propio ayuntamiento el que entra en las bases de datos del Catastro para verificar que los datos allí contenidos coinciden con los del padrón del IBI y si no es así rectificar dicho padrón para evitar evasiones fiscales de los contribuyentes de este impuesto. Una práctica que realiza, entre otros, el Ayuntamiento de La Orotava (Santa Cruz de Tenerife) según información facilitada por el ayuntamiento en fecha 13/04/2023.

CC BY SA

DOI: https://doi.org/10.51915/ret.314

utilidad para localizar situaciones de conflicto de interés o posibles ilegalidades. Además, son aquellas bases que resultan más accesibles para los ayuntamientos, en la medida que son bases del propio consistorio o, aunque sean externas, pueden acceder a ellas con relativa sencillez y que, por ello, las entidades locales pueden establecer mecanismos para empezar a utilizarlas con fines anticorrupción.

3.- El data mining como instrumento de prevención de conflictos de intereses en entidades locales: el caso de MINERVA

Junto con la utilización de las bases de datos como herramienta de prevención de la corrupción, surgen en la administración local nuevas técnicas para detectar fraudes con la utilización de datos; en concreto a raíz de la recepción de nuevos fondos europeos ha surgido la utilización de la minería de datos para encontrar corruptelas en administración.

Dicha minería de datos supone un paso más allá de la simple utilización de las bases de datos que, como se han expuesto, pueden ayudar a encontrar fraudes en las entidades. En el *data mining* se analizan un gran volumen de datos[19] para poder obtener una información de, que otro modo, pasaría desapercibida, por ello resulta de gran interés, ya que, como apunta Rodríguez González-Chaves (2022:63), dicha minería de datos permitiría prevenir y detectar la corrupción y corroborar la eficacia de las políticas públicas. Así mismo, en palabras de Valles Bento (2019:32) el análisis masivo de datos supone "la última frontera" para conseguir una mayor innovación, eficiencia y transparencia en la administración pública.

La utilización de la prospección de datos personales como herramienta de prevención de la corrupción ha llegado a las entidades locales españolas a través de la gestión de los citados fondos europeos que se han destinado a los estados miembros para paliar los efectos de la pandemia del COVID-19. En concreto, fue a través de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia (PRTR). Dicha norma establece en el anexo III.C como medidas de prevención de la

[19] El hecho de que se analicen grandes volúmenes de información no implica necesariamente un descuido de la normativa de protección de datos, de hecho, en el ámbito de la certificación, el estándar ISO/CEI 13249-6:2006, revisado y confirmado por última vez en 2021 y por el que se regula la tecnología de la información, contempla en su apartado 6 la certificación del *data mining*. En este sentido, Viguri Cordero (2020: 162) recuerda que se trata de un proceso que permite demostrar el cumplimiento efectivo del nivel de seguridad apropiado y permite proporcionar por parte de la entidad local garantías suficientes en el cumplimiento de la normativa de protección de datos vigente.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

corrupción en la gestión de los citados fondos la utilización de la minería de datos, junto con el uso de otras bases de datos o sistemas de puntuación de riesgos[20].

Por tanto, ello supone un reconocimiento expreso a que, en efecto, las técnicas de minería de datos pueden ayudar notoriamente en la prevención de conflictos de intereses de los expedientes que gestionen las entidades locales relacionados con el PRTR. Si bien, conforme al art. 6.4 de la citada Orden HFP/1030/2021: "La elección de las medidas de prevención y detección se deja a juicio de la entidad que asuma la responsabilidad de gestión", en consecuencia, la posibilidad de que una entidad local incluyera la prospección de datos en sus medidas antifraude para la tramitación de dichos fondos se trataba solo de una opción.

Ahora bien, esta situación de optatividad que tenían los ayuntamientos para poder aplicar o no técnicas de prospección de datos para prevenir fraudes en los fondos del PRTR, cambió a raíz de la disposición adicional centésima décima segunda de la Ley 31/2022, de 23 de diciembre, de Presupuestos Generales del Estado para el año 2023 (LPGE 2023) que establece que el Ministerio de Hacienda y Función Pública deberá establecer un procedimiento para realizar dicha minería de datos. De tal modo, ha sido la Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia, la que ha establecido la herramienta MINERVA de *data mining* como necesitaría cuando se gestionan subvenciones y contratos dentro de dicho PRTR. De tal modo, al utilizarse preceptivamente dicha herramienta de minería de datos se puede localizar a tiempo los conflictos de intereses que, frecuentemente, suele producirse en los ayuntamientos y, como apunta Campos Acuña (2022), evitar así la suspensión del procedimiento o incluso el reintegro de fondos del PRTR.

MINERVA tiene en cuenta diferentes bases de datos para realizar dicha tarea de prospección, en concreto la DA112ª de la LPGE 2023 que establece que se tomarán en cuenta datos de la titularidad real de personas jurídicas que consten en la Agencia Estatal de Administración Tributaria (AEAT) y los obtenidos a través de Convenios

[20] En concreto, en el apartado 1.d.i.C del anexo III.C de la Orden HFP/1030/2021, de 29 de septiembre, se establece que se pueden establecer mecanismos de prevención de conflictos de intereses consistentes en la: "Comprobación de información a través de bases de datos de los registros mercantiles, bases de datos de organismos nacionales y de la UE, expedientes de los empleados (teniendo en cuenta las normas de protección de datos) o a través de la utilización de herramientas de prospección de datos («data mining») o de puntuación de riesgos (ARACHNE)".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

con los Colegios de Notarios y Registradores[21]. Por tanto, al utilizar dichas bases de datos gracias a MINERVA se pueden identificar posibles conflictos de intereses como ahora un concejal que tenga participaciones en una empresa y conste dicho dato en la AEAT (al tributar, por ejemplo, los rendimientos de la empresa en el Impuesto sobre la Renta de las Personas Físicas) y dicho concejal sea el órgano de contratación en un expediente en el que es licitador dicha empresa, ya que en dicho supuesto debería abstenerse conforme el art. 23.2.e LRJSP. Junto con la información sobre la AEAT, se utilizará la información sobre los Colegios de Registrados y de Notarios, algo que dependerá de la suscripción del correspondiente convenio, por lo que hasta que ello se produzca dicha herramienta de minería de datos solo utilizará la base de datos de le AEAT para encontrar posibles conflictos.

Así mismo, dicha DA112ª no deja claro si la herramienta MINERVA solo pueden utilizar la bases de datos de la AEAT y las de los colegios para localizar conflictos, ya que dicha disposición establece que se harán uso de los datos de titularidad real de personas jurídicas "entre otros" contenidos en las bases de datos citadas. Por tanto, *a priori,* de la literalidad del texto se deduce la posibilidad de utilizar más datos que, simplemente, la titularidad real indicada, pero dentro de las bases referidas. Si ello es así y no se permite a dicha herramienta de *data mining* hacer uso de otras bases de datos supondría desaprovechar el potencial de la aplicación, en la medida en que podría cogerse datos de otras bases de datos de titularidad estatal, como por ejemplo de la Tesorería General de la Seguridad Social, que también permitiría localizar posibles conflictos de intereses en la gestión de los fondos del PRTR.

Cuando una entidad local utiliza MINERVA, la herramienta le devuelve un resultado indicando si se han detectado o no banderas rojas[22]. Se entiende la bandera roja como una situación de riesgo de existencia de un conflicto de interés (como señala el preámbulo de la Orden HFP/55/2023), una terminología que también se utilizó en el apartado 2.ii.B del anexo III.C de la Orden HFP/1030/2021 al establecer que se podía incluir como elementos de detección del fraude la existencia de dichas banderas rojas, que como apunta Ochsenius Robinson (2019) puede ser un riesgo emergente.

[21] En concreto, el apartado Cuatro, párrafo tercero de la DA112ª de la LPGE 2023 establece que MINERVA hará uso de las siguientes bases de datos para su tarea de *data mining*: "Para la identificación de las relaciones o vinculaciones la herramienta contendrá, entre otros, los datos de titularidad real de las personas jurídicas a las que se refiere el artículo 22.2.d).iii) del Reglamento (UE) 241/2021, de 12 febrero, obrantes en las bases de datos de la Agencia Estatal de Administración Tributaria y los obtenidos a través de los convenios suscritos con los Colegios de Notarios y Registradores".

[22] El procedimiento concreto se detalla en el artículo 5 de la citada Orden HFP/55/2023, de 24 de enero.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

Si bien, el hecho de que se detecte una bandera roja no implica necesariamente que exista un fraude, simplemente se trata de un indicio de que quizás un determinado asunto puede necesitar de una atención adicional para confirmar o descartar un determinado fraude, como pueda ser, por ejemplo, que se adjudiquen contratos a familiares del órgano de contratación. Por ello MINERVA advierte de si existen dichas banderas como una situación de riesgo a considerar donde podría existir un conflicto de interés.

En efecto, la identificación por la herramienta MINERVA de una bandera no supone necesariamente la existencia de un fraude, ya que la citada Orden HFP/55/2023 que la regula establece en primer lugar, que de aparecer una bandera roja (por haberse detectado un posible conflicto entre el órgano decisor afectado y otra persona externa a la administración que es licitador o simplemente interesado en el expediente administrativo) se deberá poner en conocimiento la existencia de dicha bandera al decisor afectado para que valore si debe abstenerse o no en el plazo de dos días. Como primera opción, el interesado puede abstenerse conforme el art. 23 LRJSP si, en efecto, considera que el posible conflicto de interés que ha localizado MINERVA es real y procede que dicho empleado o cargo público no participe de dicho asunto. En segundo lugar, existe la opción de que el decisor afectado considere que, a pesar de la bandera roja detectada, realmente no existe un conflicto de interés del que procesa abstenerse y, ante ello, será el superior jerárquico el que deba decidir en última instancia si acepta la participación de dicha persona en el proceso o le ordene la abstención. A este respecto, deberá tomar en consideración los argumentos que haya indicado el interesado, la información que haya adoptado MINERVA y también la opinión del Comité Antifraude de la entidad local[23].

De tal forma, se concede así a dicho Comité Antifraude un papel más protagonista en la detección de posibles conflictos de intereses en la gestión de los fondos europeos, al exigirle un informe cada vez que se detecte una bandera roja y el interesado decida no abstenerse. De hecho, la Orden que regula MINERVA da por hecho que todas las administraciones que gestionaban fondos del PRTR tenían un Comité Antifraude cuando la Orden HFP/1030/2021, que establecía las medidas a adoptar sobre dichos fondos ni siquiera incluye en su articulado el término de dicho Comité. En efecto, como comenta Bernal Blay (2023), se da por hecho que los comités antifraude existen cuando la normativa no obligaba hasta la fecha a ello y, como apunta el autor, hay administraciones que en lugar de crearlo han redistribuido las funciones de seguimiento de los planes antifraude entre las unidades gestoras.

[23] La Secretaría General de Fondos Europeos del Ministerio de Hacienda y Función Pública ha preparado la Guía práctica para la aplicación de la Orden HFP/55/2023 para facilitar a las administraciones públicas como utilizar adecuadamente la aplicación MINERVA y dicho documento sirve de gran utilidad, entre otros aspectos, para conocer qué pasos deben seguirse ante la aparición de una bandera roja.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

En definitiva, parece que la Orden HFP/55/2023 ha otorgado unas funciones a un Comité que quizás no existe en todas las entidades decisoras de fondos del PRTR y ello, sin duda, dificultará poder atender mejor las incidencias de banderas rojas que detecte MINERVA.

Respecto al procedimiento de actuación ante MINERVA no podemos dejar de mencionar la existencia no solo de que se detecten banderas rojas, sino también banderas negras. Se trata de una terminología nueva (que no se incluía en la Orden HFP/1030/2021sobre medidas antifraude en fondos del PRTR) y que el art. 5.c de la Orden HFP/55/2023 define como una situación en la que: "no existe información sobre riesgo de conflicto de interés para el/los siguiente/siguientes participantes, por tratarse de una entidad/entidades sobre la cual/las cuales no se dispone de datos". Ante dicha situación la Orden prevé que se siga el procedimiento de art. 7 de la misma, donde se habilita a solicitar a las personas de que las no se dispone de información que la faciliten para verificar la titularidad real. De esta manera, se realiza una verificación manual de los titulares reales de los licitadores del contrato o solicitantes de subvenciones cuando aparece dicha bandera negra y no se disponen de datos, con el fin de que la ausencia de información no sea aprovechada para ocultar un conflicto de interés que pueda desembocar en un fraude en las entidades locales que gestionan estos fondos europeos.

4.- Dificultades y retos en materia de protección de datos para emplear las bases de datos y el data mining como herramienta antifraude

Sin duda, existen herramientas y posibilidades para utilizar las bases de datos y el data mining para prevenir actuaciones corruptas en la administración local. Si bien, uno de los principales retos que debe tener en cuenta las entidades locales para poder utilizar dichas bases de datos y la minería de datos con fines anticorrupción es cómo conciliar dicho uso con la normativa sobre protección de datos personales.

Respecto a las diferentes bases de datos que se han indicado en este artículo (que contienen información que la entidad local podría utilizar para prevenir la corrupción) algunas de ellas plantearían algunos problemas para poder utilizar la información contenida con dichos fines al no ser bases con información pública, nos referimos al registro de entrada y salida del ayuntamiento y al registro de personal. En principio, utilizar dichos datos para prevenir la corrupción en la forma indicada podría chocar con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), por no existir un consentimiento expreso del interesado para utilizar dichos datos con tales fines, algo que conforme el art. 6 LOPDGDD resultaría exigible.

A pesar de dicha ausencia de consentimiento del interesado podría hacerse uso de la información de dichas bases con fines anticorrupción si se ampara en el art. 8.2

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

LOPDGDD, que sería utilizar dichos datos con fines de interés público[24]. Sin duda, se considera que no existe mayor fin público que prevenir la corrupción en las administraciones, algo que según Cerrillo Martínez (2011:279) debe producirse no solo para castigar los actos fraudulentos, sino también para prevenirlos, lo que, en nuestra opinión, se conseguiría especialmente con el uso de las bases de datos con fines anticorrupción. Si bien, el citado precepto 8.2 LOPDGDD exige que, para entender que se hace uso legítimamente de datos personales con fines de interés público, debe conferirse por una competencia atribuida por una norma de rango legal y ello es lo que plantería más inconvenientes. No encontramos en la LRBRL, principal norma que atribuye competencias a las entidades locales, referencia alguna a que deben evitar la corrupción en sus actuaciones y esto hace que resulte difícil de cumplir dicho requisito.

De hecho, con la Orden HFP/1030/2021, que regulaba las medidas que debían adoptar las administraciones gestoras de los fondos del PRTR, se establecían como medidas de prevención de conflicto de intereses en el apartado 1.d.i.C del anexo III.C de la citada Orden la comprobación de datos de expedientes de empleados, pero teniendo en consideración la normativa sobre protección de datos. En consecuencia, parece claro, en todo caso, que debe respetarse la LOPDGDD, y no parece que dicha Orden en sí sea título suficiente para poder consultar los datos en el registro de personal con fines anticorrupción, ya que lo sería si dicho precepto se hubiera incluido en una norma con rango de ley, porque así se cumpliría el requisito del art. 8.1 LOPDGDD que permite el uso de datos si lo autoriza una disposición legislativa[25]. En consecuencia, si incluso no parece que exista suficiente amparo normativo para poder usar la base de datos del registro de personal del ayuntamiento para identificar conflictos de intereses en la gestión de fondos PRTR, todavía parece más improbable que el consistorio pueda hacer uso de dicha base de datos de personal o de otra como el registro de entrada y de salida como herramienta para encontrar fraudes en el resto de los expedientes administrativos del ayuntamiento sin incumplir la LOPDGDD.

[24] El art. 8.2 LOPDGDD establece en concreto: "El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley".

[25] En concreto, el art. 8.1 de la LOPDGDD establece cómo puede usarse unos datos personales sin consentimiento del interesado si es para el cumplimiento de una obligación prevista en una norma con rango de ley: "El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

Por tanto, si realizamos una interpretación restrictiva de la LOPDGDD resultaría aconsejable no usar los datos de las bases de datos del registro de personal y del registro de entrada y salida del consistorio con fines anticorrupción, ya que no parece cumplirse plenamente los requisitos de la LOPDGDD y no haber consentimiento del interesado para utilizar los datos con dichos fines[26]. Si bien, en aras de garantizar la protección del interés general, constitucionalmente previsto en el art. 103 CE, instrumentar vías para poder hacer uso de dichas bases resultaría más que aconsejable para el uso de dichos datos de las citadas bases para prevenir actuaciones corruptas.

Es más, supongamos que, eventualmente, se identifica por un ayuntamiento un conflicto de interés entre un concejal y un licitador de un expediente donde es el órgano contratante dicho concejal y ello se hace sin consultar ninguna base datos, sino simplemente con la información que obra en el expediente de contratación (por ejemplo, por verse en la información aportada por el licitador al expediente que unos de los socios o miembros del órgano de administración de la entidad licitante es dicho concejal). Ante dicha circunstancia resultaría ilógico que la administración hiciera caso omiso a la situación y no atendiera a dicho conflicto, ya que ello, sin duda, iría en contra del interés general. Por tanto, resulta también incongruente y contrario al interés general que, disponiendo el ayuntamiento de información sobre los participantes de un expediente en sus bases de datos de personal y del registro de entrada y salida del consistorio, no pueda consultar dichos datos cuando tramite el expediente si lo hace exclusivamente con fines antifraude, para localizar, por ejemplo, un conflicto de interés o una prohibición para contratar.

Así mismo, también cabría la opción de plantearse si con los datos de dichas bases eventualmente no solo se descubre un fraude que origina una infracción administrativa, sino que incluso se pueda detectar un ilícito penal y, por tanto, si a partir de entonces sería de aplicación ya no la LOPDGDD sino la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (LOPDIP). Si bien, de nuevo nos encontramos ante un callejón sin

[26] El requisito consentimiento que, como apunta García Mahamut (2018:68 y 74), se debe obtener con un proceso cada vez más fortalecido, ya que se produce una reforma sin precedentes en la regulación de la protección de datos, con lo que, sin duda, dicho requisito del consentimiento es fundamental que se cumpla plenamente, por ello, queda claro que no parece que se cumpla en este caso en referencia a la posibilidad de usar los datos personales de dichas bases con fines antifraude, ya que los interesados no aportaron los datos con dichos fines y no parecen cumplirse el resto de requisitos que permite la LOPDGDD para poder usar dichos datos.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

salida, en la medida en que el art. 4 LOPDIP[27] no incluye a las entidades locales entre los sujetos legitimados para dichas actuaciones de prevención o detección del fraude, por lo que dicha norma tampoco ampara a los ayuntamientos para usar dichas bases de datos con dichos fines. De todos modos, téngase en cuenta que la LOPDIP solo sería de aplicación cuando se investiguen asuntos penales, pero no simples fraudes administrativos que quizás no están tipificados como delitos pero puedan suponer un fraude que atente contra el buen gobierno de la entidad local (por ejemplo, una abstención que debió producirse en un cargo electo y no se efectuó).

Con todo, consideramos que debería ponerse más énfasis en permitir el uso de las bases de datos con fines anticorrupción, y como no parecen del todo legitimadas las entidades locales conforme a la LOPDGDD y a la LOPDIP para poder hacerlo, sería aconsejable una actualización normativa para permitir de forma expresa el uso de dichas bases de datos con fines antifraude. Además, los esfuerzos en este sentido deben producirse para cumplir principalmente con la LOPDGDD, ya que ello permitiría detectar en los expedientes administrativos tanto fraudes de tipo penal como administrativo (ya que la LOPDIP solo actúa sobre cuestiones penales).

Téngase en cuenta que una actuación para permitir cumplir con la normativa de protección de datos resulta altamente factible en la medida en que ya se hizo para implantar la minería de datos de MINERVA, puesto que al establecerse dicha herramienta por la DA112ª de la LPGE 2023 se incluyó en un título legal, la LPGE 2023, que permitía el uso de las bases de datos que consulta MINERVA sin infringir la normativa sobre protección de datos, en concreto, cumpliendo el requisito del art. 8.1 LOPDGDD. Por tanto, de hacerse dicha actualización normativa supondría una oportunidad para hacer uso de datos que ya están a disposición del ayuntamiento y que la LOPDGDD no permitiría, en principio, utilizarlo para identificar posibles fraudes locales. En este sentido, Gil González (2017) destaca cómo la existencia de un gran volumen de datos que tenemos a disposición pueden aportar beneficios económicos o sociales que no deben ser desaprovechados y, por ello, deben buscarse opciones para "flexibilizar el tratamiento de datos, al mismo tiempo que se protegen los derechos de los individuos", lo que en este caso planteado pasaría por

[27] El art. 4.1. LOPDIP establece: "En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades: a) Las Fuerzas y Cuerpos de Seguridad. b) Las Administraciones Penitenciarias. c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria. d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo". En consecuencia, no se incluye a las entidades locales como legitimadas para el uso de las bases de datos que tienen a su alcance para prevenir fraudes de corrupción que posteriormente puedan convertirse en delitos penales.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

una reforma normativa en aras de permitir un uso de las bases de datos con fines anticorrupción.

Por lo que respecta a las implicaciones en materia de protección de datos del registro de intereses de cargos electos del art. 75.5 LRBRL, partimos de que la norma estatal establece el carácter público de dichas declaraciones[28], lo que en principio permitiría poder utilizar sin mayores límites los datos de dichas declaraciones de intereses con fines anticorrupción, en la medida en que si los datos son públicos por exigencia normativa, la LOPDGDD no impediría su uso por una entidad local, en la medida en que incluso cualquier ciudadano podría consultarlos.

Ahora bien, lo cierto es que en materia de declaraciones de intereses de ediles locales existen diferentes normas que han modulado esta exigencia estatal, de manera que no debe publicarse todo el contenido de las declaraciones, sino que debe salvaguardarse, por ejemplo, la información sobre localización exacta de bienes, tal y como establece la normativa autonómica valenciana[29] o la propia normativa estatal de transparencia[30].

Por tanto, en la práctica nos encontramos ante un registro de intereses que, aun teniendo carácter público, no siempre toda la información que se publicita es la que se inscribe en el registro. En consecuencia, respecto a aquella información que de los registros de intereses que no se publicite nos podríamos encontrar con el mismo límite anteriormente citado de la ley de protección de datos, donde la ausencia de una norma legal que habilite a su uso (art. 8.1 LOPDGDD) o la falta de una competencia municipal sobre la materia (art. 8.2 LOPDGDD) podría impedir a la entidad local utilizar dichos datos para detectar fraudes en expedientes.

---

[28] Así lo establece el art. 75.7, párrafo cuarto y quinto LRBRL: "Las declaraciones anuales de bienes y actividades serán publicadas con carácter anual, y en todo caso en el momento de la finalización del mandato, en los términos que fije el Estatuto municipal. Tales declaraciones se inscribirán en los siguientes Registros de intereses, que tendrán carácter público".

[29] En concreto, el art. 3 del Decreto 191/2010, de 19 de noviembre, del Consell, por el que se regulan las declaraciones de actividades y de bienes de los miembros de las corporaciones locales de la Comunitat Valenciana establece: "En relación con los bienes patrimoniales, la declaración que se publique será únicamente comprensiva de la situación patrimonial de os representantes locales y miembros no electos de las juntas de gobierno local, omitiéndose aquellos datos referentes a su localización y salvaguardando la privacidad y seguridad de sus titulares, constando los datos que se indican en el anexo".

[30] El art. 8.1.h LTBG establece: "Las declaraciones anuales de bienes y actividades de los representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

Ahora bien, consideramos que a pesar de dicho límite en materia de protección de datos, en el caso de las declaraciones del registro de intereses sí estaría legitimada la entidad local para usar los datos de dicho registro con fines anticorrupción, en la medida en que, en efecto, la información de dicha declaración de intereses se ha aportado a la entidad local justamente con el fin de evitar que los ediles incurran en conflictos y para que pueda identificarse posibles fraudes durante el ejercicio de su cargo. De hecho, como apunta González i Ballesteros (1999:2201) dicho registro se encuentra "al servicio de la transparencia de la gestión municipal y para la depuración de responsabilidades civiles y penales que impliquen a miembros consistoriales", por lo que parece lógico que se puedan utilizar sus datos para localizar posibles fraudes en expedientes administrativos.

De hecho, en este sentido se pronunciaron el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos (AEPD) en dictamen conjunto[31] al indicar que respecto a la información de cargos electos deberá darse publicidad y por tanto será consultable: "en cuanto el acceso a la información contribuya a un mejor conocimiento de los criterios de organización y funcionamiento de las instituciones o a la asignación de los recursos, cabrá considerar la existencia de un interés público prevalente sobre los derechos a la protección de datos y a la intimidad". Un criterio que mantiene el informe del Gabinete Jurídico de la AEPD núm. 373514/2015[32] al indicar que dar adecuada publicidad de la información contenida en dichos registros de intereses permite verificar que la actuación del cargo público no ha recibido influencias externas indebidas que le afecte a su independencia que debe mantener en el ejercicio de la función pública.

En consecuencia, parece justificado que la entidad local pueda hacer uso de los datos de los concejales contenidos en el registro de intereses para poder detectar fraudes en los expedientes administrativos, en la medida en que, en efecto, ello ayudará a identificar posibles conflictos de intereses que entorpecerían un correcto funcionamiento de las instituciones conforme al interés general.

Menos problemática en materia de protección de datos plantea el uso de algunas bases de datos como la Base de Datos Nacional de Subvenciones, ya que en dicha herramienta deben publicarse de forma abierta determinada información sobre las subvenciones de forma que cualquier ciudadano pueda acceder, incluida una administración que quiere utilizar dichos datos para prevenir fraudes en sus

[31] Dictamen conjunto del Consejo de Transparencia y Buen Gobierno y de la Agencia Española de Protección de Datos elaborado en fecha 25 de marzo de 2015 a raíz de la Solicitud 1/2015 – Oficina para la Ejecución de la Reforma de la Administración.

[32] Informe del Gabinete Jurídico de la Agencia Española de Protección de Datos n.º373514/2015.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

expedientes. En efecto, como apunta Lanza Suárez (2019:177) dicha BDNS facilita el cumplimiento de los principios de publicidad y transparencia sin mayor coste para las entidades locales. En concreto, conforme al art. 7.8 del Real Decreto 130/2019, de 8 de marzo, por el que se regula la BDNS y la publicidad de las subvenciones y demás ayudas públicas podrán consultarse las subvenciones concedidas a una persona física durante el año de concesión y el siguiente y para el caso de que el beneficiario es persona jurídica durante el año de concesión y los cuatro años siguientes. Por tanto, aunque la información no se publica con carácter indefinido, ello supone un régimen de publicidad suficiente para que las entidades locales puedan hacer uso de la BDNS con fines para detectar fraudes en sus expedientes.

De igual forma, no se plantea problemática respecto al ROLECE, que conforme el art. 344 LCSP se trata de un registro de acceso abierto por lo que su consulta es pública y permite a los ayuntamientos comprobar los datos con fines antifraude. Con los datos contenidos en el Registro de la Propiedad ocurre de forma semejante, ya que se permite el acceso a los datos y por tanto el ayuntamiento puedo utilizarlo para evitar fraudes, ya que el art. 221 del Decreto de 8 de febrero de 1946 por el que se aprueba la nueva redacción oficial de la Ley Hipotecaria[33], el acceso a dicho Registro está permitido y todavía con más justificación para un empleado municipal que accede al mismo para verificar, por ejemplo, la propiedad de un inmueble con el que va a suscribir un derecho real o a firmar un convenio el ayuntamiento.

En referencia al Registro Mercantil, el mismo también tiene carácter público conforme el art. 12 del Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil, lo que permite acceder a datos que pueden resultar de especial interés para los consistorios locales para detectar posibles conflictos de intereses en expedientes, como ahora los administradores de una mercantil. Si bien, como habíamos avanzado, el Registro Mercantil no proporciona datos sobre los socios de las personas jurídicas inscritas en el mismo, con lo cual ésto supone un límite importante ya que permitiría identificar más prohibiciones para contratar del art. 71 LCSP.

Por lo que respecta a la información catastral, existe determinados datos no protegidos donde no existen límites de acceso, como por ejemplo la localización o

[33] El art. 221 del Decreto de 8 de febrero de 1946 por el que se aprueba la nueva redacción oficial de la Ley Hipotecaria establece: "Los Registros serán públicos para quienes tengan interés conocido en averiguar el estado de los bienes inmuebles o derechos reales inscritos. El interés se presumirá en toda autoridad, empleado o funcionario público que actúe por razón de su oficio o cargo".

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

a la superficie de un inmueble[34], de manera que conforme el art. 52.1 del Real Decreto Legislativo 1/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Catastro Inmobiliario, cualquier persona podría acceder, lo que también permitiría a las entidades locales utilizar dicha información con fines antifraude. Si bien, la principal información que las entidades locales pueden necesitar del Catastro para poder sacar más provecho a su base de datos es poder conocer a los titulares de las parcelas para así poder encontrar, en su caso, posibles conflictos de intereses entre dichos titulares y funcionarios o cargos públicos locales. Ahora bien, la información sobre los titulares de la información catastral se tratan de datos catastrales protegidos que, según el art. 51 del citado Real Decreto Legislativo 1/2004, solo se pueden consultar por parte de personas afectadas, propietarios de parcelas colindantes, titulares o cotitulares de derechos y herederos, por lo que parece que el ayuntamiento no podría acceder legítimamente a dichos datos para comprobaciones antifraude en principio, ya que no entraría en las categoría de dicho precepto legal y conforme el art. 8.1 LOPDGDD resultaría necesario dicha legitimación por ley para tener el pleno acceso. Ello supone, por tanto, otra ocasión desaprovechada para que las entidades locales puedan utilizar al máximo el potencial de las bases de datos a su alcance para localizar fraudes y corruptelas en sus expedientes.

5.- Conclusiones

Ha quedado patente el potencial de las bases de datos y del *data mining* como herramienta que pueden utilizar las entidades locales para identificar fraudes en expedientes administrativos. Suponen, por tanto, una nueva opción para detectar actuaciones que puedan alejarse del interés general en la administración local, poniendo especial énfasis en la detección de conflictos de intereses que tan frecuentemente se originan en los ayuntamientos.

Si bien, la falta de exigencia legal para la utilización de las bases de datos o de las técnicas de *data mining* hace que este se trate todavía de un ámbito a explotar por los ayuntamientos. Téngase en cuenta que actualmente solo es de obligada aplicación las técnicas de minería de datos en la gestión de los fondos europeos, derivados del Plan de Recuperación, Transformación y Resiliencia. Ahora bien, esta técnica de prospección de datos podría ser ampliada a otros asuntos tramitados por las entidades locales. Para ello, resultaría conveniente una futura regulación legal que ampliara la posibilidad de la utilización del *data mining* en el resto de los

[34] De hecho, si consultamos la página web del Catastro nos indica que es de público acceso la siguiente información no protegida: localización del inmueble, referencia catastral, superficie, uso o destino, clase de cultivo o aprovechamiento, calidad de la construcción o cartografía.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

expedientes municipales, en aras de prevenir conflictos de intereses y conseguir una mejor gestión pública.

De igual forma sucede con la utilización por parte de las entidades locales de las bases de datos a su alcance para encontrar posibles fraudes, ya que si existe voluntad política y técnica de querer utilizarlas con dichos fines se consigue verdaderamente evitar conductas corruptas que de otras formas hubieran pasado desapercibidas, por lo que supone una auténtica oportunidad de avanzar en el buen gobierno por las entidades locales. Ahora bien, el principal reto en la utilización de estas bases de datos por las entidades locales con fines antifraude se basa en los límites en materia de protección de datos personales.

De tal modo, se ha destacado la necesaria futura actuación normativa en materia de protección de datos para poder utilizar los datos de determinadas bases a las que tiene acceso al ayuntamiento y que, al no ser públicas en su totalidad, los datos contenidos no siempre tienen un amparo normativo suficiente para utilizar los datos para localizar fraudes. En concreto, resultaría aconsejable una disposición legislativa que expresamente permita utilizar con fines antifraude las bases de datos que tiene el propio ayuntamiento (como el registro de personal o el registro entrada y de salida de documentos) y así cumplir con el requisito del artículo 8.1 LOPDGDD.

Asimismo, en otras bases de datos externas al ayuntamiento, pero a las que éste tiene acceso, si se produjera la actualización de la normativa sectorial de aplicación para potenciar el uso de las mismas por los ayuntamientos se conseguiría identificar numerosos fraudes. Así pues, por ejemplo, si se produjera una actualización de la normativa catastral que permitiera a los ayuntamientos acceder a la titularidad de los inmuebles para identificar fraudes en materia, por ejemplo, de recaudación de tributos locales, resultaría muy aconsejable para evitar la pérdida de caudales públicos. También, en lo referido al uso del ROLECE, si se efectúa una revisión legislativa de la LCSP para obligar a los órganos de contratación a verificar posibles prohibiciones para contratar en todo tipo de contratos (no solo en el procedimiento abierto simplificados en los que resulta obligatorio actualmente) se evitarían numerosos fraudes que actualmente pasan desapercibidos. Por tanto, puede resultar altamente aconsejable una puesta al día de la normativa correspondiente que permita a los ayuntamientos usar las bases de datos a su disposición que contienen datos que no tienen carácter público con fines anticorrupción.

Si bien, consideramos que el reto principal no se encuentra en la protección de datos, sino en la voluntad de las entidades locales de querer utilizar dichas bases de datos para evitar fraudes. En efecto, actualmente, como se ha expuesto, ya existen bases de datos o determinados datos de algunas bases que son públicos o que el ayuntamiento tendría legitimación suficiente para utilizarlos con fines anticorrupción y, en la práctica, las entidades no utilizan todavía para detectar fraudes. De hecho,

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

los dirigentes públicos podrían utilizar los códigos de buen gobierno para autoexigir a sus consistorios locales la utilización de los bases de datos con fines anticorrupción, dentro de los límites normativos existentes, si bien ello no parece encontrarse en los principales códigos de las entidades locales de este país[35]. No podemos obviar que implantar un uso de dichas bases de datos para vigilar la corrupción en las entidades locales supondría una mayor carga de trabajo del personal de los consistorios, aunque no consideramos que ello suponga una gran dificultad para los consistorios, en tanto en cuanto la consulta de datos al ser telemática puede ser ágil y el beneficio a obtener, que es evitar fraudes públicos, es altísimo.

Todo ello supone, por tanto, una oportunidad perdida, puesto que las entidades locales están desaprovechando una información que está a su disposición y que serviría para evitar la corrupción en sus expedientes. Y es que debemos concebir esas técnicas como verdaderos instrumentos de calidad de la democracia que satisfagan la confianza legítima en la ciudadanía; y ello con respecto a una acción de buen gobierno que no refleje meras preocupaciones estéticas, sino verdaderamente éticas y de regeneración democrática[36].

Es por ello que la clave en el éxito de la utilización de dichas bases de datos y del *data mining* en las entidades locales para evitar el fraude está, principalmente, en el compromiso político con el buen gobierno local, de forma que verdaderamente los dirigentes públicos apuesten por utilizar dichas técnicas anticorrupción que les permita lograr una administración local que verdaderamente satisfaga el interés general constitucionalmente previsto.

[35] Si analizamos algunos de los principales códigos de buen gobierno en España no encontramos referencias al uso de bases de datos para prevenir la corrupción, por ejemplo, véase el modelo Código de Buen Gobierno de la Federación Española de Municipios y Provincias del 2015. El código del Ayuntamiento de Barcelona tampoco establece medidas como tal, si bien en su art. 13.c indica que el consistorio dará apoyo a aquellas entidades que reutilicen los datos de contratación para controlar la adjudicación y ejecución de contratos, por lo que en la práctica sí supone una primera iniciativa del consistorio local para empezar a apostar por el uso de las bases de datos con fines anticorrupción, aunque sea con el apoyo a una entidad externa que realizará tales funciones.

[36] Tal como ha advertido JIMENA QUESADA (2022:158).

CC BY SA

DOI: https://doi.org/10.51915/ret.314

Bibliografía

ARAGÓN AMUNÁRRIZ, F. 2020 "La colaboración del Catastro con las Entidades Locales". *El Consultor de los Ayuntamientos*, núm. 4.

ARNALDO ALCUBILLA, E. 2009. "Las elecciones locales en la doctrina de la Junta Electoral Central: actividades de campaña, régimen de incompatibilidades, renuncia de los electos y sustitución, moción de censura, consultas populares y otras cuestiones". *Anuario del Gobierno Local,* núm. 1: 517-541.

BERNAL BLAY. M.A. 2023. *El control de los conflictos de interés en los procedimientos administrativos que ejecutan fondos del Plan de Recuperación, Transformación y Resiliencia*. Online: Observatorio de Contratación Pública. Disponible en: https://www.obcp.es/opiniones/el-control-de-los-conflictos-de-interes-en-los-procedimientos-administrativos-que (consultado el 15/03/2023).

BLANCO LÓPEZ, F. 2022. *Prohibición de contratar. Las Administraciones Públicas incumplen la LCSP,* Online: Observatorio de Contratación Pública Española. Disponible en: https://www.obcp.es/opiniones/prohibicion-de-contratar-las-administraciones-publicas-incumplen-la-lcsp (consultado el 5/3/2023).

CAMPOS ACUÑA, M.C. 2015. "Códigos éticos y buen gobierno local en la Ley de Transparencia". *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* núm. 9:72-87.

CAMPOS ACUÑA, M.C. 2021. "*Data Mining* contra la corrupción en los fondos europeos". *Cinco Días* de *El País*. Publicado el 8/11/2021. Disponible en: https://cincodias.elpais.com/cincodias/2021/11/03/legal/1635951205_097450.html (consultado el 13/6/2023).

CAMPOS ACUÑA, M.C. 2022. "Nuevas obligaciones sobre conflicto de intereses en el PRTR. *Data mining* en la LPGE para el año 2023". *El Consultor de los Ayuntamientos*, núm. 27/12/2022.

CERRILLO I MARTÍNEZ, A. 2011. "Transparencia administrativa y lucha contra la corrupción en la Administración local". *Anuario del Gobierno Local,* núm. 1: 277-313.

FERNÁNDEZ AJENJO, J.A. 2019. "La política del fraude de subvenciones y su incidencia en las Entidades Locales". *El Consultor de los Ayuntamientos*, núm. 1.

FIBLA NICOLAU, C. 2010. "Causas de incompatibilidad y abstención del personal al servicio de las entidades locales (autoridades y funcionarios". *Cuadernos de derecho local,* núm. 23:166-191.

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

GALINDO CALDÉS, R. 2019. "Prohibición de contratar e incompatibilidades de los concejales". *Cuadernos de Derecho Local,* núm. 51: 119-139.

GARCÍA MAHAMUT, R. 2018. "El derecho fundamental a la protección de datos. El Reglamento (UE) 2016/679 como elemento definidor del contenido esencial del artículo 18.4 de la Constitución". *Corts: Anuario de derecho parlamentario*, núm. extra 31: 59-80.

GIL GONZÁLEZ, E. 2017. "Big data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?". *Diario La Ley*, núm. 9050.

GONZÁLEZ I BALLESTEROS, J. 1999. "El registro de intereses de los miembros de las Entidades Locales: cuestiones no explícitas en la legislación vigente". *El Consultor de los Ayuntamientos*, núm. 13.

JIMENA QUESADA, L. 2022. "Democracia de calidad y exigencias de buen gobierno tras la crisis pandémica". *Revista Galega de Administración Pública*, vol. 1, núm. 63: 155-182.

LANZA SUÁREZ, P. 2019 "40 meses a bordo de la Base de Datos Nacional de Subvenciones", *El Consultor de los Ayuntamientos*, núm. 1.

MARÍN PÉREZ, A. 2007. "El nuevo régimen del registro de intereses de las corporaciones locales", *El Consultor de los Ayuntamientos,* núm. 20: 3246.

MOLINA MESA, J. 2016. *Dimensión del gasto subvencional, control sobre su aplicación y responsabilidad de gestores y beneficiarios.* Granada: Universidad de Granada.

OCHSENIUS ROBINSON, I. 2019. "El control en la contratación pública", en OCHSENIUS ROBINSON, I. (Dir.), *Mecanismos de control, mejora y calidad en la contratación pública*. Madrid: El Consultor de los Ayuntamientos.

PUYAL SANZ, P. 2018. "El Catastro como instrumento de lucha contra el fraude inmobiliario: el valor de referencia de mercado". *Crónica Tributaria,* núm. 169: 139-176.

RODRÍGUEZ GONZÁLEZ-CHAVES, F. 2022. "El uso del *data mining* en los programas de compliance para evitar la corrupción". *El Consultor de los Ayuntamientos*, núm. 2.

TOMÁS MALLÉN, B. 2022. "Derechos fundamentales y *Drittwirkung* en perspectiva multinivel: desarrollos recientes en el Derecho europeo". *Revista de Derecho Político*, núm. 115: 207-235.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 17. Número Extraordinario 2023
www.revistatransparencia.com

CC BY SA

Sección Estudios y Artículos
Las bases de datos y el *data mining* como herramientas contra la corrupción en la administración local
por Jaime Clemente Martínez
Págs. 299-328
DOI: https://doi.org/10.51915/ret.314

VALLES BENTO. L. 2019. "Aplicación de inteligencia artificial y big data en el control de la Administración Pública y en el combate a la corrupción: la experiencia del gobierno brasileño". *Revista General de Derecho Administrativo,* núm. 50: 1-37.

VIGURI CORDERO, J. (2021): "La adopción de instrumentos de certificación como garantía eficiente en la protección de los datos personales", *Revista Catalana de Dret Públic,* núm. 62 :60-176.