Expediente Nº: E/02410/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el Área de Gobierno de Participación Ciudadana, Transparencia y Gobierno Abierto (Ayuntamiento de Madrid), en virtud de denuncia presentada por Doña ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 16 de marzo de 2017, tuvo entrada en esta Agencia un escrito remitido por Doña ***A.A.A.,*** en el que expone lo siguiente:

"Es objeto de esta denuncia la actuación llevada a cabo por el Ayuntamiento de Madrid para desarrollar el proceso participativo llevado a cabo entre el 13 y 19 de febrero de 2017.

Es sabido que los datos del padrón municipal se pueden utilizar por parte de los ayuntamientos sin violentar los derechos de protección de datos cuando tengan la finalidad de desarrollar competencias municipales conferidas por la Ley de Bases de Régimen Local y demás normativa de desarrollo. No cabe duda que las consultas para la realización de votaciones por parte de los vecinos, constituye una competencia municipal pero para que quede garantizada la protección es necesario que el uso de los datos personales que se incluyen en el padrón (nombre, domicilio, DNI, fecha de nacimiento, etc.), sea realizado dentro de los márgenes que garantizan el carácter confidencial de los mismos.

Uno de los requisitos para un uso correcto de estos, es que el acceso a los mismos sea realizado por personal funcionario, pues solo de ese modo y por las peculiares características de este personal derivadas de sus deberes de actuación (artículos 52 a 54 del Estatuto Básico del Empleado Público aprobado por Real Decreto Legislativo 5/2015), se entiende respetado el carácter confidencial de los mismos tal y como se establece en el artículo 53.2 del Real Decreto 1690/1986, de 11 de julio, por el que se aprueba el Reglamento de Población y Demarcación de las Entidades Locales.

Pues bien, el Ayuntamiento de Madrid a juicio de la que suscribe no ha respetado en el proceso participativo que he señalado, el carácter confidencial de los datos, incurriendo en una clara violación del derecho a la protección de datos personales, dado que para desarrollar el mismo ha permitido el acceso a los datos del padrón a personas voluntarias, que no ostentan la cualidad de funcionario, sin que se entienda a estos efectos que la firma de un compromiso de estos colaboradores, constituya un mecanismo que garantice el carácter confidencial de los mismos.

Lo aquí manifestado pudo comprobarse porque participé en dicho proceso votando presencialmente. Se me pidió el DNI y el voluntario encargado de la labor, accedió mediante una tablet a mis datos personales del padrón municipal. Presencié asimismo comentarios de los citados voluntarios sobre la edad de una persona que me había precedido en la votación.

Asimismo en la apertura de sobres, para recuento de la votación puede haberse

producido una vulneración del derecho a la protección de datos, en tanto personal voluntario accede a datos como nombre, DNI y domicilio de la persona que ha votado.

Como acreditación de lo manifestado, señalo la siguiente dirección de correo explicativa de las circunstancias del desarrollo del proceso participativo https://diario.madrid.es/.....

Por todo lo expuesto formulo la presente denuncia a fin de que se dé inicio al procedimiento oportuno con la finalidad de que recaiga la correspondiente sanción sobre el Ayuntamiento de Madrid ante la vulneración del derecho a la protección de datos personales incluidos en el padrón municipal y en evitación de que tal situación se vuelva a producir en los siguientes procesos participativos que el citado ente local ha anunciado que tiene intención de desarrollar"

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Los representantes del Ayuntamiento de Madrid manifiestan que en el proceso de participación ciudadana se realizaron básicamente los siguientes tratamientos de datos:

1. Envío de cartas a los ciudadanos

   En enero de 2017, se envió una carta a todos los ciudadanos empadronados en Madrid, con edad superior a 16 años, invitándoles a votar dos propuestas ciudadanas.

   La votación se podía realizar por correo postal, de forma presencial o a través de la web Decide Madrid.

   Para la extracción de los datos personales necesarios para personalizar la carta y el sobre prefranqueado para el voto por correo, se utilizó el sistema de información ePOB, que trata los datos del padrón municipal de habitantes, y sólo accedieron a esta información personal funcionario del Ayuntamiento de Madrid.

   La impresión y personalización de los documentos los realizó la entidad IMPAORSA Soluciones Gráficas Avanzadas, con la que se ha firmado un acuerdo de confidencialidad y protección de datos

   La personalización de los sobres para el voto por correo lo realizó la entidad Tompla Industria Internacional del Sobre, S.L., con quien el Ayuntamiento de Madrid ha suscrito igualmente un acuerdo de confidencialidad y protección de datos.

2. Proceso de Votación Presencial

   Se realizó en urnas situadas en diversos centros públicos entre los días 13 a 19 de febrero de 2017.

   Las mesas de votación estaban atendidas por al menos dos personas, un presidente y un vocal, todos ellos voluntarios o colaboradores y exhibían un cartel informativo para los ciudadanos detallando los datos que deben facilitar, y

el responsable del tratamiento.

Los colaboradores eran 982 usuarios de la web Decide Madrid y los voluntarios fueron seleccionados de entre los inscritos en Voluntarios por Madrid, en total fueron 149 personas.

Todos ellos recibieron un curso previo en el que se les concienció sobre la confidencialidad en el acceso a los datos personales y suscribieron un documento de colaboración comprometiéndose a guardar secreto respecto a toda información, con datos personales o no, que como consecuencia de su participación en el proceso hubieran podido acceder.

Estos documentos se conservan archivados, y son exhibidos a los inspectores por los responsables del Ayuntamiento, verificando que se encuentran firmados por los voluntarios y colaboradores.

Para regular este proceso de participación ciudadana, el Ayuntamiento aprobó, mediante decreto, el manual de funcionamiento de las mesas de participación en los procesos convocados.

En el manual se describe el proceso protocolizado, detallando las labores y tareas que se encomiendan a los participantes, incluyendo las pautas para identificar a los ciudadanos.

Este manual se entregó a los voluntarios y colaboradores y recoge en el anexo IV el modelo de acuerdo de confidencialidad que debía firmar cada uno.

Los días de la votación se dotaron a los voluntarios con una Tablet para controlar la participación ciudadana.

Cada Tablet tenía conexión segura a Internet y, a través de este medio, a la aplicación Decide Madrid. Se creó un perfil de acceso a esta aplicación para controlar el voto mediante un interfaz específico.

El servicio de informática asignó este perfil a los voluntarios, todos ellos usuarios de Decide Madrid, para permitir la validación de la identidad del votante y si podía votar.

Para ello debía incorporar en el programa el DNI, u otro medio oficial de identificación, y el año de nacimiento. El sistema informaba si el ciudadano estaba empadronado y era mayor de 16 años, y en caso afirmativo, para cada opción que se votaba, se optaba por una de las siguientes respuestas:

Puede votar

Ya ha participado en esta votación

Se adjunta como documento copia de las instrucciones para la utilización de la Tablet por parte de los colaboradores/voluntarios.

Finalizada la votación los voluntarios y colaboradores procedieron al recuento y levantaron un acta con el resultado.

3. Votación por correo

Se han recibido aproximadamente 150.000 votos por correo; los sobres se custodiaron cerrados con llave en dependencias municipales y fueron trasladados a Matadero para su recuento.

El traslado lo realizó la entidad Mudanzas Zarza S.A., con la que se suscribió un compromiso de confidencialidad por cada uno de los dos portes realizados.

4. Recuento

   En las instalaciones municipales de Matadero, se procedió al recuento de los votos por correo, en fecha 20 de febrero de 2017.

   Los encargados del recuento de estos votos eran voluntarios y ciudadanos que se presentaban libremente para colaborar.

   Los voluntarios ya habían firmado el compromiso de confidencialidad para estar presentes en las mesas de votaciones; los ciudadanos que se presentaron voluntarios firmaron este documento antes de tener acceso a los datos personales contenidos en los sobres con votos.

   Para esta labor se les asignaba una Tablet para que realizaran el recuento final y escrutinio.

   Una vez finalizado el recuento se procedió a la destrucción de los sobres, siguiendo el protocolo de destrucción del material utilizado en la votación.

Los representantes del Ayuntamiento aportan copia del protocolo de destrucción y de actas de eliminación de residuos que según indican corresponden a los sobres, papeletas y documentación con datos identificativos de los participantes en la votación por correo

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

El artículo 126.1, apartado segundo, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal establece:

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

II

Los hechos denunciados en el presente expediente se concretan en que en el proceso de participación ciudadana, realizada por el Ayuntamiento de Madrid entre los días 13 y 19 de febrero de 2017, el acceso a datos del Padrón Municipal de Habitantes se realizó por colaboradores y voluntarios no funcionarios que, a pesar de haber suscrito un compromiso de confidencialidad, no garantiza la confidencialidad del acceso a los datos.

La obligación de guardar secreto es uno de los principios en materia de protección de datos, que viene establecido en el artículo 10 de la LOPD, que dispone:

"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. En el supuesto denunciado, obliga a todos los funcionarios o las personas que no ostenten la condición de funcionarios, que accedan a los datos de los ciudadanos que se encuentran en el fichero "Padrón de Habitantes"

Este deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene un *"instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos"* (Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

La Sentencia de la Audiencia Nacional, Sección 1ª de la Sala Contencioso-administrativa, de fecha 18 de junio de 2009, indica lo siguiente con referencia al deber de secreto:

<<Por lo tanto, resulta que no se ha acreditado que se haya producido ninguna forma de infracción del deber de secreto pues aunque, es cierto que la documentación no estuvo correctamente custodiada y no era razonable que las historias clínicas viajaran en un camión con el resto de escombros de la demolición de un hotel, la realidad es que ninguna violación del secreto se ha producido y nadie ha llegado a tener noticia de la documentación clínica que, al parecer, sigue custodiada en las cajas en

cuestión cuya fotografía ha aportado la parte recurrente.

Esta Sala tiene establecido como la infracción del deber de secreto es una infracción de resultado en la que lo relevante es que se llegue a producir la divulgación de un secreto, no siendo relevante (a los efectos de la violación del deber de secreto) con la simple omisión de medidas de seguridad.

En la sentencia correspondiente al recurso 471/2008 se expuso expresamente esta cuestión razonando del siguiente modo: <<La infracción tipificada en el art. 44.3.g) es una infracción de resultado que exige que los datos personales sobre los que exista un deber de secreto profesional -como aquí ocurre en relación con el número de la cuenta corriente- se hayan puesto de manifiesto a un tercero, sin que pueda presumirse que tal revelación se ha producido. Efectivamente, la Agencia Española de Protección de Datos en su resolución se limita a poner de manifiesto que el sistema de cierre, mediante ventanilla transparente, de los sobres utilizados por el Banco para realizar determinadas comunicaciones a sus clientes pudiera dar lugar a que determinados datos personales contenidos en esas comunicaciones puedan ser conocidas por terceras personas respecto de las que deba mantenerse el secreto. No prueba sin embargo que los datos fueran efectivamente conocidos por dichos terceros. Estaríamos, por tanto, como sostiene el recurrente, ante una posible infracción de medidas de seguridad -que es una infracción de actividad- pero no ante la infracción que se le imputa que exige la puesta en conocimiento de un tercero de los datos personales.

Por otro lado, tampoco se deduce de la observación del sobre que fue aportado junto con la denuncia -ya abierto y rotos sus mecanismos de confidencialidad- que la revelación del número de la cuenta corriente pudiera producirse (al estar roto tal comprobación no es posible) y en el propio Acta de Inspección levantada el 21 de noviembre de 2007 se hace constar que los inspectores solicitaron el acceso a los sobres utilizados por OPEN BANK para remitir documentación a sus clientes por Postal Express, verificando que a través de la ventanilla que contiene no es posible visualizar el número de cuenta bancaria del cliente. Por tanto, además de no haberse acreditado la revelación de datos personales a persona alguna, tampoco se ha acreditado que el sistema de ensobrado utilizado por la parte recurrente para la realización de determinados envíos postales permita que dicha revelación sea posible.>>

Aplicando ese mismo criterio, resulta que en el caso presente no se ha llegado a producir divulgación alguna por lo que no se justifica la imposición de la sanción derivada de una revelación de secretos que no se llegó a producir.>>

La Sra. ***A.A.A.*** denuncia que durante el proceso de participación ciudadana descrito en los antecedentes de hecho no se ha garantizado la confidencialidad de los datos a los que han accedido los voluntarios que han participado en los mismos. Hay que señalar que el Ayuntamiento de Madrid ha realizado un curso previo formativo

dirigido a los voluntarios y colaboradores durante el cual les ha tratado de concienciar sobre la confidencialidad que debían guardar sobre los datos que conociesen en el desarrollo de su labor; además les hizo firmar a todos ellos un documento en el que se comprometían a guardar secreto respecto a toda la información que conociesen como consecuencia de la colaboración que realizarían.

Esto es, el Ayuntamiento de Madrid realizó una labor formativa previa. Como se ha indicado, la infracción del deber de secreto es una infracción de resultado. Junto con la denuncia no se ha presentado ningún indicio de que se haya producido vulneraciones al deber de secreto por parte de los voluntarios y participantes en el proceso de votación presencial realizado en el mes de febrero de 2017 por el Ayuntamiento de Madrid.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **AREA DE GOBIERNO DE PARTICIPACION CIUDADANA, TRANSPARENCIA Y GOBIERNO ABIERTO (AYUNTAMIENTO DE MADRID)** y ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos