



Procedimiento nº.: E/04163/2017

ASUNTO: Recurso de Reposición Nº RR/00102/2018

Examinado el recurso de reposición interpuesto por Doña **A.A.A.**, contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/04163/2017, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 3 de enero de 2018, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/04163/2017, procediéndose al archivo de actuaciones en aplicación del principio de presunción de inocencia.

Dicha resolución, que fue notificada a la recurrente en fecha 10 de enero de 2018, según aviso de recibo que figura en el expediente.

SEGUNDO: Doña **A.A.A.** ha presentado, en fecha 10 de febrero de 2018, con registro de entrada en esta Agencia del día 16 del mismo mes y año, recurso de reposición, fundamentándolo básicamente en que se han incumplido las normas y doctrina que han de ser observadas en la valoración de la prueba, en lo relativo al supuesto cumplimiento del artículo 12 de la LOPD, ya no se ha referenciado lo esencial del contrato de prestación de servicios. No existe protocolo municipal y el Reglamento interno que existe en la Administración Pública es ajeno a una entidad privada. La documentación presentada por el Ayuntamiento de Santiago no cumple lo establecido en el artículo 12 de la LOPD. Principalmente la reutilización de los datos por parte de la empresa contratada en el año 2016 durante el año siguiente incumple la obligación de destruir o devolver la documentación generada.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP).

II

El recurso de reposición insiste en los hechos denunciados y que fueron contestados en la Resolución de archivo ahora recurrida, de la forma siguiente:

<<La denuncia se concreta, en primer lugar en que el Ayuntamiento de Santiago de Compostela ha contratado a una empresa para la recogida y tratamiento

de datos de vecinos relacionados con el Proyecto de Presupuestos Participativos sin que exista contrato de prestación de servicios entre el mencionado Ayuntamiento y la empresa que lo realiza: Ciudadania rede de aplicacions sociais, Sociedad Cooperativa Galega, ni para el año 2016 ni para el 2017. En segundo lugar, denuncia que la empresa contratada utiliza los datos obtenidos en el año 2016 para el proyecto del año 2017 ya que los relativos al año 2016 no fueron devueltos ni destruidos al finalizar el servicio. En tercer lugar, denuncia que el procedimiento de recogida de datos de los ciudadanos no prevé medidas para acreditar la identidad y el consentimiento de los participantes, ya que únicamente se solicita el DNI y la fecha de nacimiento y las alertas instauradas por la empresa para evitarlo tampoco son eficaces ya que en algunos casos se puede remitir confirmación a la dirección email incorporadas en el momento de recabar los datos en la web.

En relación al primero de los hechos denunciados, el artículo 12 de la LOPD “acceso a datos por cuenta de terceros”, establece lo siguiente:

“1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”.

El citado artículo 12.1 de la LOPD permite que el responsable del fichero habilite el acceso a datos de carácter personal por parte de la entidad que va a prestarle un servicio –encargado del tratamiento- sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión de datos. La LOPD exige que el acceso a datos por cuenta de terceros figure reflejado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, y prevé unos contenidos mínimos, tales como seguir las instrucciones del responsable del tratamiento, no utilizar los datos para un fin distinto, no comunicarlos a otras personas, estipular las medidas de seguridad del artículo 9 y, cumplida la prestación, destruir los datos o proceder a su devolución al responsable del tratamiento.

En el presente caso, ha quedado constatado que existe formalizado contrato



de prestación de servicios firmado por el Ayuntamiento de Santiago de Compostela y la entidad Ciudadania, firmado el día 17 de junio de 2016, para desarrollar el Proyecto del Presupuesto Participativo 2016, en el que constan los requisitos establecidos por el citado artículo 12 de la LOPD y que se ha venido desarrollando de conformidad con lo detallado en los Antecedentes de esta Resolución.

En fecha 19 de mayo de 2017 se firmó un nuevo contrato de prestación de servicios entre el Ayuntamiento de Santiago de Compostela y la entidad Ciudadania, que fue nuevamente la adjudicataria del Proyecto del Presupuesto Participativo para el año 2017.

En segundo lugar, la denunciante señala que la empresa contratada utiliza los datos obtenidos en el año 2016 para el proyecto del año 2017 ya que los relativos al año 2016 no fueron devueltos ni destruidos al finalizar el servicio.

Hay que señalar que durante estas actuaciones previas de investigación el Ayuntamiento de Santiago de Compostela ha informado que al finalizar el primer contrato, Ciudadania remitió un CD-ROM al Ayuntamiento con los diez ficheros que habían gestionado. El censo de personas participantes en el Proyecto del año 2016 continúa con los datos personales para el año siguiente, salvo que los afectados hubiesen solicitado la baja del censo o no estén empadronados ya en Santiago de Compostela.

IV

En tercer lugar, se ha denunciado que el procedimiento de recogida de datos de los ciudadanos no prevé medidas para acreditar la identidad y el consentimiento de los participantes, ya que únicamente se solicita el DNI y la fecha de nacimiento y las alertas instauradas por la empresa para evitarlo tampoco son eficaces ya que en algunos casos se puede remitir confirmación a la dirección email incorporadas en el momento de recabar los datos en la web.

El artículo 6.1 de la LOPD dispone que “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. El apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en el 6.1 estableciendo que: “No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento...”

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre (F. J. 7 primer párrafo) “consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un



particular (...)."

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

La LOPD además de sentar el anterior principio de consentimiento, regula en su artículo 4 el principio de calidad de datos. El apartado 2 del citado artículo 4, dispone: "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos." Las "finalidades" a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley. Conforme a dicho precepto los datos sólo podrán tratarse cuando "sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido." En consecuencia, si el tratamiento del dato ha de ser "pertinente" al fin perseguido y la finalidad ha de estar "determinada", difícilmente se puede encontrar un uso del dato para una finalidad "distinta" sin incurrir en la prohibición del artículo 4.2 aunque emplee el término "incompatible".

La citada Sentencia del Tribunal Constitucional 292/2000, se ha pronunciado sobre la vinculación entre el consentimiento y la finalidad para el tratamiento de los datos personales, en los siguientes términos: "el derecho a consentir la recogida y el tratamiento de los datos personales (Art. 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aún cuando puedan ser compatibles con estos (Art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por ley, pues el derecho fundamental a la protección de datos personales no admite otros límites. De otro lado, es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (Art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia."

De lo expuesto cabe concluir que la vigente LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales en lo relativo a los requisitos del



consentimiento, de la información previa a éste y de las finalidades para las que los datos pueden ser recabados y tratados.

En el supuesto denunciado, es el afectado el que cumplimenta el formulario con sus datos y es informado de la utilización de los mismos a partir de la política de privacidad que ha de aceptar. Por tanto, el afectado consiente de manera inequívoca al tratamiento de sus datos cuando los incluye en la plataforma Participare. Por otro lado, el Ayuntamiento ha incluido “alertas” para evitar la suplantación de la personalidad.

Las “alertas” para evitar la suplantación de personalidad, existentes en el año 2016, eran contactar telefónicamente o por mail con el participante con el objeto de comprobar la identidad, validándose únicamente en el caso de que éste lo confirme cuando se producían estas circunstancias:

Una IP con tres o más registros en el periodo de 30 minutos

Una IP con más de 100 registros.

Una IP con diez registros sospechosos, entendiendo como sospechoso aquellos que coinciden entre el nombre y apellidos, nombre de usuario y dirección de correo electrónico.

*Los datos de la denunciante se registraron desde la dirección IP ***IP.1, el día 19 de octubre de 2016. Ese mismo día se realizaron 17 registros con datos de ciudadanos desde esa dirección IP.*

Por ello, se contactó telefónicamente con la denunciante en fecha 19 de octubre de 2016 a las 13:40 y al no confirmar los datos se rechazó de la base de datos Participare.

Dos días después, el Ayuntamiento recibió una llamada de la denunciante, a las 11:30, en la que solicitaba explicaciones sobre el uso indebido de su identidad, solicitando la dirección IP desde la que se habían proporcionado sus datos a la Plataforma de Participare, facilitándole la mencionada dirección IP.

En el año 2017 y para mejorar el sistema de alertas, se ha rebajado el límite de activación de 100 registros grabados desde una misma dirección IP a 20 registros.

En consecuencia, tras las investigaciones realizadas y estudiada la documentación aportada por el Ayuntamiento de Santiago de Compostela se ha constatado que ese Consistorio firmó contratos de prestación de Servicios con la entidad Ciudadania para la realización del Programa de Presupuestos Participativos, verificando la autenticidad del consentimiento de cada formulario presentado conteniendo datos personales.>>

III

El hecho de que no se detalle todas y cada una de las cláusulas de los contratos de prestación de servicios firmados entre ambas partes no supone, como indica la recurrente, que no consten en el expediente.

Por lo tanto, en el presente recurso de reposición, la recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

La Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por Doña **A.A.A.** contra la resolución de esta Agencia dictada con fecha 3 de enero de 2018, en el expediente de actuaciones previas de inspección E/04163/2017.

SEGUNDO: NOTIFICAR la presente resolución a Doña **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, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

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