- **Expediente N.º: PS/00361/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante), en fecha 17 de febrero de 2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el AYUNTAMIENTO DE ALBACETE con NIF P0200300B (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

En concreto, manifiesta que, al acceder a su área privada para consultar el estado en el que se encontraba la tramitación de su expediente, ha visualizado datos personales de otras personas (nombres, DNI/NIE, direcciones y teléfonos) y solicitudes de registro de otros administrados.

Junto a la reclamación aporta documentos procedentes de la sede electrónica relativos a otras solicitudes de bajas de inscripción en el Padrón Municipal de Habitantes, con datos visibles de número de registro de entrada, nombre y apellidos de la persona solicitante del procedimiento.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 22 de marzo de 2021, como consta en el acuse de recibo que obra en el expediente.

En fecha 21 de abril de 2021, se recibe en esta Agencia escrito de respuesta indicando que cuando el reclamante accede electrónicamente, (mediante uso de su certificado digital reconocido), en fecha 17-02-2021 al expediente electrónico tramitado al efecto relativo a las comunicaciones/solicitudes de bajas de inscripción en el Padrón Municipal de Habitantes correspondientes al mes de agosto de 2020, existían dentro del mismo, cinco carpetas de documentos de otras solicitudes, con los únicos datos visibles de número de registro de entrada y el nombre y apellidos de la persona solicitante en el procedimiento, (es decir, no se podía identificar a la persona en cuestión, por la disociación que existe, al no aparecer junto con su nombre y apellidos su número de DNI o pasaporte), que dado que se tratan de solicitudes de la misma

naturaleza se acumulan en expedientes que se crean al efecto con periodicidad mensual, todo ello, de conformidad con los preceptos legales de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (artículo 58) y añade que debe haber una acción posterior (consciente y deliberada) por parte de la persona que accede al expediente, de hacer clic de manera voluntaria en la pestaña de abrir cada una de las carpetas de otros ciudadanos que han presentado una instancia con el mismo propósito que el suyo, para visualizar los datos personales e identificativos, pues le aparecerán todos los que haya incluido ese interesado en su instancia: DNI/NIE/Pasaporte, dirección postal y de empadronamiento y teléfonos de contacto. Por último, añade que vienen realizando esta tramitación de expedientes de bajas/altas en el Padrón Municipal de Habitantes de este municipio de esta manera, desde el 19 de septiembre de 2016, fecha en la que se inicia la tramitación electrónica, sin que hasta la fecha hayan recibido ninguna reclamación de estas características.

TERCERO: En fecha 2 de julio de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: En fecha 18 de febrero de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por las presuntas infracciones de los artículos 5.1.f) y 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD, respectivamente.

El acuerdo de inicio fue enviado, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibido en fecha 22 de febrero de 2022, como consta en el certificado que obra en el expediente.

Notificado el citado acuerdo de inicio, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que, ante la necesidad por parte del Ayuntamiento de Albacete, de adherirse al modelo tecnológico desarrollado e implantado por la Diputación Provincial para la prestación de servicios de Administración Electrónica, la Diputación asumió la encomienda de gestión de los servicios de administración electrónica del Ayuntamiento y la colaboración técnica en materia de definición de tipologías de expedientes, formatos de intercambio e interoperabilidad, exponía además que la herramienta de Sistema de Gestión de Expedientes Electrónicos (SEGEX) es propia de la Diputación de Albacete y puesta a disposición de los distintos Ayuntamientos para facilitar la gestión de expedientes, por lo que la responsabilidad recaería sobre la propia Diputación, que a la vista de la reclamación del ciudadano, el Ayuntamiento remitió escrito a la Diputación Provincial solicitando la modificación en la configuración de los niveles de acceso establecidos por defecto por la propia herramienta y que han adoptado medidas de seguridad oportunas para mitigar el riesgo existente de acceso a datos personales de los interesados vinculados al mismo expediente, por lo que solicita el archivo de las actuaciones.

QUINTO: En fecha 12 de abril de 2022, se formuló propuesta de resolución, proponiendo:

<< Que por la Directora de la Agencia Española de Protección de Datos se imponga al AYUNTAMIENTO DE ALBACETE, con NIF P0200300B, por una infracción del artículo 5.1. f) del RGPD, conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD y por infracción del artículo 32 del RGPD, conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción den el artículo 73 apartado f) de la LOPDGDD, una sanción de apercibimiento. >>

La citada propuesta de resolución fue enviada, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibida en fecha 13 de abril de 2022, como consta en el certificado que obra en el expediente.

SEXTO: En fecha 28 de abril de 2022, la parte reclamada presentó escrito de alegaciones a la Propuesta de Resolución, en el que, en síntesis, se reiteran los argumentos ya expuestos en las alegaciones anteriores.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Consta que en fecha 17 de febrero de 2021, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, debido a una violación de seguridad de los datos personales.

SEGUNDO: Se verifica que el reclamante ha podido acceder a documentos procedentes de la sede electrónica del Ayuntamiento de Albacete relativos a otras solicitudes de bajas de inscripción en el Padrón Municipal de Habitantes, con datos visibles de número de registro de entrada, nombre y apellidos de la persona solicitante del procedimiento.

TERCERO: La parte reclamada expone que, desde la unidad de gestión del padrón de habitantes, para agilizar el procedimiento, se realiza un único expediente SEGEX en el que se acumulan las solicitudes que se realizan durante un mes de todos los interesados en darse de baja del Padrón. La causa principal de esta violación de seguridad se debe a que cada documento que se crea en dicho expediente viene configurado por defecto para que todos los interesados actuales del expediente y los que se añadan posteriormente, puedan acceder a dicho documento. La causa secundaria de la violación de seguridad se debe a que esta configuración por defecto no es cambiada de forma manual por el gestor del expediente, para que indique que sólo el interesado sea el que acceda al documento.

Asimismo, manifiesta que ha procedido a implantar las medidas correctoras adecuadas para evitar la repetición de hechos similares en el futuro. La documentación aportada se encuentra incorporada al expediente.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II

En relación con las manifestaciones efectuadas por la parte reclamada, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas no sólo fueron analizadas y desestimadas, sino que se tuvieron en cuenta para formular la Propuesta de resolución, cuyos Fundamentos de Derecho continúan plenamente vigentes, y que se resumen en lo siguiente:

"En el presente caso, la entidad reclamada es la responsable de los tratamientos de datos, toda vez que, conforme al artículo 11 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público:

"1*. La realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las Entidades de Derecho Público podrá ser encomendada a otros órganos o Entidades de Derecho Público de la misma o de distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño.*

Las encomiendas de gestión no podrán tener por objeto prestaciones propias de los contratos regulados en la legislación de contratos del sector público. En tal caso, su naturaleza y régimen jurídico se ajustará a lo previsto en ésta.

2. La encomienda de gestión no supone cesión de la titularidad de la competencia ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o Entidad encomendante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de encomienda.

En todo caso, la Entidad u órgano encomendado tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución de la encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal."

El artículo 4.7 del 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 por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos -RGPD-) define al responsable del tratamiento o responsable como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros."*

Asimismo, el citado Reglamento se refiere -en el apartado 8 de su artículo 4-, al encargado del tratamiento o encargado como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".*

En este sentido cabe recordar que la figura del encargado del tratamiento obedece a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso y tratamiento se realiza por el encargado, en nombre y por cuenta del responsable, como si fuera este mismo quien lo lleva a cabo.

El Informe 0064/2020 del Gabinete Jurídico de la AEPD ha expresado con rotundidad que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)": *"la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan".*

El artículo 5.2 del RGPD establece que «el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")». Esto significa que el responsable deberá garantizar la aplicación efectiva de los principios del tratamiento tanto en el momento de determinar los medios del tratamiento como durante el tratamiento en sí, a través de la articulación de una serie de medidas, las cuales deberán ser objeto de revisión y actualización periódica. Ello implica que el citado responsable es el que asume su propia responsabilidad dirigiendo y coordinando la materia, incluyendo la del personal que le presta servicios.

Se tiene en cuenta a estos efectos lo señalado en el siguiente considerando del RGPD:

74. "*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas."*

Sobre la infracción de falta de medidas de seguridad para el tratamiento de datos, la Audiencia Nacional señaló en diversas sentencias: (13 de junio de 2002 -recurso nº. 1.517/2001 -, 7 de febrero de 2003 -recurso nº. 1.182/2001 -, 25 de enero de 2006 -recuso nº. 227/2004 -, 28 de marzo de 2006 recurso 478/2004, 28 de junio de 2006 -recurso nº. 290/2004 -, 24 de marzo de 2015 -recurso nº. 269/2013 - y 25 de junio de 2015 -recurso nº. 90/2014), que la obligación que dimana de la implantación de medidas de seguridad en lo concerniente a los datos de carácter personal, "*no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, y por supuesto, no basta con la aprobación formal de las medidas de seguridad, ya que resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. (…)*"

Frente al riesgo de que un ciudadano que accede a su expediente pueda abrir cada una de las carpetas de otros ciudadanos que han presentado una instancia con el mismo propósito que el suyo, pudiendo visualizar datos personales e identificativos, se observa la falta de estas medidas. El Ayuntamiento tomó la decisión de acumular varios expedientes de baja en el Padrón municipal, en aplicación del artículo 57 de la Ley 39/15 (erróneamente el Ayuntamiento menciona el artículo 58). Esta decisión es propia del Ayuntamiento y no obedece al diseño de la herramienta, lo que facilitó el acceso indebido a la información de otros interesados, cuando realmente no tiene sentido acumular expedientes que, aun refiriéndose a la misma materia, son de interesados distintos. La herramienta informática permitía al personal del Ayuntamiento seleccionar qué tipo de interesados podían tener acceso al expediente. Si bien por defecto la opción es "todos los interesados", la selección se podía cambiar manualmente (lo que debió hacer el personal del Ayuntamiento en este caso). No se hizo, lo que, de nuevo, propició que "todos los interesados" tuvieran acceso. Y, como se ha señalado, "todos los interesados" eran los de todos los expedientes que, sin ningún sentido, habían sido acumulados.

Estas medidas preventivas, orientadas a garantizar la confidencialidad, integridad y disponibilidad de los datos, que han de ser instauradas, han de ser también objeto de seguimiento en su cumplimiento y efectividad, así como cuando varían las circunstancias del tratamiento, atendiendo y contemplando en su caso, cualquier incidente que pueda acontecer.

Por consiguiente, el responsable del tratamiento debe llevar a cabo un análisis de los riesgos de los tratamientos de datos, implantando las medidas técnicas y organizativas apropiadas para aplicar los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD, debiendo poder demostrar que el tratamiento es conforme con lo previsto en la citada norma.

Finalmente, entre las medidas adoptadas tras la brecha, el Ayuntamiento manifiesta que remitió escrito a la Diputación Provincial solicitando la modificación en la

configuración de los niveles de acceso establecidos por defecto por la propia herramienta. En este sentido, una mínima diligencia del Ayuntamiento tendría que haber hecho que lo solicitaran antes. Y, en todo caso, debió vigilar, caso a caso, que a cada expediente se accediera solo por los interesados en el mismo. Siendo, así las cosas, y aun cuando en el caso presente la entidad reclamada hubiera procedido, en el momento de determinación de los medios, a diseñar e implementar unas medidas acordes, ello no le eximiría de seguir siendo responsable de la efectividad de dichas medidas durante todo el tiempo en que se hubiera producido la recogida y tratamiento de los datos personales.

En el presente caso consta acreditado que los datos personales de usuarios de la herramienta de Sistema de Gestión de Expedientes Electrónicos fueron indebidamente expuestos a terceros desde el propio sistema de información, vulnerando los principios de integridad y confidencialidad, ambos establecidos en el artículo 5.1.f) del RGPD.

Por lo tanto, el incumplimiento de la normativa sobre protección de datos debe ser plenamente imputada al responsable del tratamiento, al no actuar de forma activa y eficaz en estipular y hacer efectivas las especificaciones oportunas para llevar a cabo adecuadamente en el tiempo, el tratamiento encomendado en su nombre.

En consecuencia, las alegaciones deben ser desestimadas."

III
Artículo 5.1f)

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento

1. *Los datos personales serán:*

(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, consta acreditado que datos personales de ciudadanos obrantes en la aplicación informática para la gestión del padrón municipal de habitantes fueron indebidamente expuestos a terceros, vulnerando los principios de integridad y confidencialidad, ambos establecidos en el citado artículo 5.1.f) del RGPD.

IV
Tipificación de la infracción del artículo 5.1f) del RGPD

El artículo 83.5 del RGPD dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o,

tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "Infracciones" determina lo siguiente: "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica."*

A efectos del plazo de prescripción de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente: *"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679."

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 del RGPD, arriba transcrito.

V
Artículo 32 del RGPD

Establece el artículo 4.12 del RGPD que se considera "*violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*."

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos (El subrayado es de la AEPD).

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

En el presente caso, la falta de implantación de medidas técnicas y organizativas ha provocado el acceso por terceros no autorizados a los datos alojados en el sistema de información de la sede electrónica de la parte reclamada, vulnerando con ello el artículo 32 del RGPD.

A este respecto, y tal y como ha quedado expuesto en el fundamento anterior, el Ayuntamiento tomó la decisión de acumular varios expedientes de baja en el Padrón municipal, en aplicación del artículo 57 de la Ley 39/15 (erróneamente el Ayuntamiento menciona el artículo 58). Esta decisión es propia del Ayuntamiento y no obedece al diseño de la herramienta, lo que facilitó el acceso indebido a la información de otros interesados, cuando realmente no tiene sentido acumular expedientes que, aun refiriéndose a la misma materia, son de interesados distintos. La herramienta informática permitía al personal del Ayuntamiento seleccionar qué tipo de interesados podían tener acceso al expediente. Si bien por defecto la opción es "todos los interesados", la selección se podía cambiar manualmente (lo que debió hacer el personal del Ayuntamiento en este caso). No se hizo, lo que, de nuevo, propició que "todos los interesados" tuvie-

ran acceso. Y, como se ha señalado, “todos los interesados” eran los de todos los expedientes que, sin ningún sentido, habían sido acumulados.

Finalmente, y como asimismo se expone en el fundamento anterior, entre las medidas adoptadas tras la brecha, el Ayuntamiento manifiesta que remitió escrito a la Diputación Provincial solicitando la modificación en la configuración de los niveles de acceso establecidos por defecto por la propia herramienta. En este sentido, una mínima diligencia del Ayuntamiento tendría que haber hecho que lo solicitaran antes. Y, en todo caso, debió vigilar, caso a caso, que a cada expediente se accediera solo por los interesados en el mismo. Siendo, así las cosas, y aun cuando en el caso presente la entidad reclamada hubiera procedido, en el momento de determinación de los medios, a diseñar e implementar unas medidas acordes, ello no le eximiría de seguir siendo responsable de la efectividad de dichas medidas durante todo el tiempo en que se hubiera producido la recogida y tratamiento de los datos personales.

En el presente caso consta acreditado que los datos personales de usuarios de la herramienta de Sistema de Gestión de Expedientes Electrónicos fueron indebidamente expuestos a terceros desde el propio sistema de información,

La consecuencia de esta falta de medidas de seguridad de obligado cumplimiento fue la exposición a terceros ajenos de los datos personales de ciudadanos usuarios de la sede electrónica. Es decir, los afectados se han visto desprovistos del control sobre sus datos personales.

En este caso la búsqueda en internet, por ejemplo, del nombre, apellidos, DNI o correo electrónico de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular.

Esta posibilidad supone un riesgo añadido que se ha de valorar en el estudio de gestión de riesgos y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento quien debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por el responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

VI
Tipificación de la infracción del artículo 32 del RGPD

El artículo 83.4 del RGPD dispone lo siguiente:

“4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) *las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43."*
(…)

A efectos del plazo de prescripción de las infracciones, el artículo 73 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas graves"*, establece lo siguiente:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.4 del RGPD, arriba transcrito.

VII

Responsabilidad

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

VIII
Sanción

El artículo 83.7 del RGPD añade:

"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."

El ordenamiento jurídico español ha optado por no sancionar con multa a las entidades públicas sino con apercibimiento, tal como se indica en el artículo 77.1. c) y 2. 4. 5. y 6. de la LOPDGDD:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica."

Con arreglo a dichos criterios, se estima adecuado sancionar con apercibimiento a la parte reclamada, por infracción del artículo 5.1 f) del RGPD, tipificada en el artículo

83.5 del RGPD, y por infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

IX
Medidas

El artículo 58.2 del RGPD dispone*: "Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;"

Asimismo, procede imponer la medida correctiva descrita en el artículo 58.2.d) del RGPD y ordenar a la parte reclamada que establezca las medidas de seguridad adecuadas para que se adecúen los tratamientos a las exigencias contempladas en los artículos 5.1.f) y 32 del RGPD, impidiendo que se produzcan situaciones como la que ha dado origen a la reclamación.

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: SANCIONAR con APERCIBIMIENTO al AYUNTAMIENTO DE ALBACETE, con NIF P0200300B, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

SEGUNDO: SANCIONAR con APERCIBIMIENTO al AYUNTAMIENTO DE ALBACETE, con NIF P0200300B, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

TERCERO: REQUERIR al AYUNTAMIENTO DE ALBACETE que implante las medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares.

CUARTO: NOTIFICAR la presente resolución a AYUNTAMIENTO DE ALBACETE.

QUINTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-050522

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