



Resolución RPS-20/2022

[Proc. PS-2021/020 - Expte. RCO-2020/020]

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Asunto: Resolución de procedimiento sancionador contra el Ayuntamiento de Jerez de la Frontera por una presunta infracción de la normativa de protección de datos personales.

HECHOS

Primero. El 4 de junio de 2020, [XXXXX], el reclamante), interpuso reclamación ante el Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) contra el Ayuntamiento de Jerez de la Frontera, (en adelante, el órgano reclamado), por una presunta infracción de la normativa de protección de datos personales.

En la citada reclamación se exponía lo siguiente:

“Con fecha [dd/mm/aa] estuve implicado en un accidente de tráfico en las calles próximas a mi domicilio [...] tras el que se personó la policía local y fui trasladado a las dependencias de la jefatura de la policía local con el fin de ser sometido a la [realización de pruebas]. Tras la realización de las mismas abandoné las dependencias de la policía local a las [hh:mm] horas de la tarde.

En la mañana del día [dd/mm] recibo una llamada del periodista [se cita nombre] perteneciente a [nombre del medio de comunicación] realizándome preguntas en relación al atestado policial y datos concretos del incidente que me recalcaaban estaban contenidos en el atestado. Le dije que no entendía cómo podía disponer de esa información ya que, ni yo mismo como persona afectada tenía esa documentación y que eso no era legal, a lo que no me respondió. Tras esta llamada y consultando los medios de comunicación, comprobamos que aparecieron publicadas en dos medios de comunicación digitales imágenes del documento del expediente de la instrucción con



información que ni siquiera había sido trasladada al juzgado. Específicamente aparecieron imágenes de documentos de la instrucción en:

A. *www.[nombre del medio de comunicación].es* bajo el titular *[datos del atestado policial]*.

B. *www.[nombre del medio de comunicación].es* bajo el titular *[datos del atestado policial]* DOCUMENTO N° 2f. (Se desconoce la hora de publicación).

A raíz de estas publicaciones otros medios de comunicación y personas se hicieron eco de las mismas, bien compartiendo la noticia o haciendo referencia en publicaciones propias a los datos que se habían revelado del atestado policial. Entre otros merece destacar:

C. Diversos medios de comunicación, periodistas y personas individuales que se hicieron eco y compartieron las noticias anteriormente indicadas con contenido secreto de la instrucción del expediente del accidente.

D. Publicaciones de ámbito local, provincial, regional y nacional con referencias a datos del atestado policial revelado destacando el *[nombre del medio de comunicación]*".

Se adjuntaban a la reclamación diversos recortes de prensa que relataban los hechos que han motivado la reclamación.

Segundo. En virtud de los artículos 37 y 65 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), con fecha 30 de julio de 2020 se dio traslado de la reclamación al Delegado de Protección de Datos del Ayuntamiento de Jerez de la Frontera (en adelante, el DPD) para que, en el plazo máximo de un mes, comunicara la respuesta dada a la reclamación y, en su caso, las actuaciones realizadas en relación con la misma.

En respuesta al requerimiento anterior, la Sra. Alcaldesa de Jerez de la Frontera, con fecha 31 de agosto de 2020, remitió a este Consejo informe del Responsable del Servicio Municipal de Informática, así como informe del Jefe de la Policía Local.

En el informe emitido por el Responsable del Servicio Municipal de Informática se indicaba que:

"[...] No obstante desde este Servicio de Informática, debemos indicar que no existen mecanismos que garanticen la seguridad total de una filtración de un documento, ya





que este estará expuesto entre otros a posibles escaneados o fotografías de los mismos, lo que sí podemos asegurar es que el acceso a las unidades de red donde se almacenan los documentos está restringida exclusivamente a las personas que ha sido autorizadas para ello por parte del responsable del servicio pertinente”.

Por su parte, en el informe del Jefe de la Policía Local se señalaba que:

“Con el objetivo de aclarar esta posible filtración de los datos de carácter personal del reclamante e intentar comprobar si la misma pudo producirse en estas dependencias policiales, el día [dd/mm], tras conversación con la Señora Alcaldesa, esta Jefatura tomó las siguientes acciones:

Le comuniqué al Inspector [se cita nombre], Jefe del servicio de turno de tarde del [dd/mm], dos cuestiones:

- Relación de los agentes que trabajaron en Inspección de Guardia en turno de tarde y noche del día [dd/mm] y turno de mañana del [dd/mm].

- Que comprobara si en el ordenador de “Inspección de Guardia 1” se encontraba en la bandeja de correos enviados, el correo que se envió el [dd/mm] al correo del Inspector [se cita nombre] y con nombre de archivo adjunto [se cita nombre de archivo]. que contenía el documento escaneado de parte del atestado en el que figuraba [el reclamante].

[...]

De la segunda cuestión, confirma que el correo con el archivo adjunto continúa en la bandeja de correos enviados a las [hh/mm] del día [dd/mm].

El día [dd/mm] recibo informe de los agentes intervinientes en la redacción del atestado como instructor y secretario con DPI [nnnnn] y [nnnnn], en el que manifiestan las medidas de seguridad que aplicaron, conforme a las órdenes recibidas del Inspector Jefe del servicio [se cita nombre], DPI [nnnnn]. Comunican en el informe que el Inspector Jefe del servicio les solicitó copia de lo actuado, enviando correo electrónico al referido Inspector a las [hh/mm] del día [dd/mm].

[...]



Con fecha *[dd/mm/aa]* se recibe informe de los agentes integrantes del turno de noche del día *[dd]*, que manifiestan que tenían conocimiento trasladado por los compañeros del turno de tarde, de que se encontraban las diligencias del atestado físico relativo al *[el reclamante]* en la carpeta correspondiente al turno de tarde y que recibieron instrucciones de especial cuidado en su custodia. Según refiere el agente DPI *[nnnnn]* procede a extraer el atestado de la carpeta del turno de tarde y guardarla en su taquilla personal que se encuentra en la misma Inspección de Guardia, asegurando que no salieron de la misma en todo el servicio. Durante el siguiente relevo se hizo entrega de la documentación al turno entrante.

También con fecha *[dd/mm]* se recibe informe de los agentes que prestaron servicio en el turno de mañana del día *[dd/mm]* DPI *[nnnnn]*, *[nnnnn]* y *[nnnnn]*, manifestando que habían recibido la información y las instrucciones sobre el atestado de referencia comunicando las novedades al Subinspector *[nnnnn]* (Jefe de la Inspección de Guardia). Igualmente comunican que durante el servicio no compareció ninguno de los implicados en el atestado pendientes de comparecer, por lo que el atestado no fue modificado. Aseguran igualmente, que durante el servicio en ningún momento la Inspección de Guardia quedó sin personal presente.

El día *[dd/mm]* se recibe informe del Jefe de Inspección de Guardia DPI *[nnnnn]*, el cual manifiesta que a las *[hh/mm]* horas del día *[dd/mm]* fue alertado por el Oficial DPI *[nnnnn]*, de servicio en la Inspección de Guardia de que aparecía publicado en el periódico *[nombre del medio de comunicación]* fotos del atestado relativo a la *[persona]* en cuestión. Que procedió a realizar averiguaciones, obteniendo información del agente DPI *[nnnnn]*, instructor del atestado, de que el Inspector DPI *[nnnnn]* le había dado orden de enviarle el documento en la tarde del día *[dd/mm]*, lo cual se realizó.

El día *[dd/mm]*, se recibe informe del Inspector DPI *[nnnnn]*, el cual se encontraba de Jefe de Servicio el día *[dd/mm]* en el turno de tarde, exponiendo que cuando tuvo conocimiento de lo sucedido, lo puso en conocimiento del Intendente- Jefe de la Policía. Que incluso antes de iniciarse la tramitación de las diligencias dio instrucciones precisas a los agentes para tratar de cuidar la privacidad del implicado, tal como le trasladó el Intendente-Jefe. Ante la solicitud recibida solicita a inspección le manden los documentos del atestado, lo cual le remiten desde Inspección de Guardia a su correo a





las [hh/mm] horas del día [dd/mm]. Se reenvía la información al Intendente- Jefe a las [hh/mm] del mismo día.

[...]

El que suscribe, a solicitud de la Sra. Alcaldesa y como tal Jefa del Cuerpo de la Policía Local, le remite copia de las diligencias a las [hh/mm] del día [dd/mm].

Dado que además del atestado físico, existía un documento de parte del mismo escaneado electrónicamente, se solicita el día 21 de mayo de 2020 al Director del Servicio Municipal de Informática del Ayuntamiento de Jerez, que efectúe averiguaciones sobre el posible reenvío del archivo del correo enviado al Inspector [nnnnn] a algún otro correo desde el equipo de "Inspección de Guardia", o si puede haber sido copiado a través de pendrive u otros dispositivos desde ese equipo, respondiendo el día [dd/mm] a las [hh/mm]. literalmente: «en relación al correo recibido y una vez consultado con el departamento de sistema, te informo que no es posible con los medios técnicos que contamos en la actualidad, averiguar la trazabilidad del fichero al que haces referencia, una vez analizados los recursos de la red asignada a Policía Local, así como el equipo asignado al usuario que se nos indica, no hemos encontrado ningún archivo con el nombre referenciado, por lo que no es posible averiguar nada sobre el mismo. Igualmente indicarte que siempre es posible sacar una o varias "fotos" de la pantalla que se está visualizando, sin que esto llegue a dejar rastro.»

Tras los informes de todos los agentes en los que manifiestan haber custodiado de forma correcta y profesional el atestado y del informe del servicio de informática, en el que no puede precisar, con los medios que cuenta, si se hubiera podido acceder al mismo por algún medio técnico, no es posible concretar la autoría y el método que dio lugar a la aparición de parte del atestado en algunos medios de comunicación.

Informar que los hechos referenciados están siendo investigados, al parecer por denuncia del [el reclamante], por la Fiscalía de esta ciudad, habiendo sido citados a declarar 15 agentes de este Cuerpo incluido la Jefatura, así como el Sr. Delegado de Seguridad y el responsable del sistema informático municipal. Todos en calidad de testigos.

En cuanto a las medidas que se han tomado reseñar:



- Propios informes requeridos a los actuantes
- Informes requeridos al responsable del sistema de informática municipal.
- Recordatorio a toda la plantilla de la Orden de Jefatura 153/16 referida a la obligación policial del secreto profesional.
- Petición al servicio de informática municipal del refuerzo de medidas de seguridad de los documentos electrónicos generados en esta Jefatura”.

Se adjuntaba al informe copia de un artículo del medio “[nombre del medio de comunicación]” del día [dd/mm/aa].

Tercero. Una vez que la reclamación inició su tramitación con arreglo al procedimiento establecido en el Título VIII de la LOPDGDD, y en virtud del artículo 67.1 de la misma, con fecha 16 de septiembre de 2020 el director del Consejo ordenó el inicio de actuaciones previas de investigación a los efectos de lograr una mejor determinación de los hechos y circunstancias que justificaran la tramitación de un posible procedimiento sancionador.

Cuarto. En el marco de dichas actuaciones y con el objeto de completar la información relacionada con los hechos denunciados, el 10 de junio de 2021, desde el Consejo se requirió al DPD para que, en el plazo de veinte días hábiles, remitiera información y documentación sobre las actuaciones llevadas a cabo en relación con la reclamación; en particular, se solicitaba, entre otra documentación:

- Determinación concreta de la actividad de tratamiento relacionada con la reclamación e identificación del responsable de dicho tratamiento, así como de los posibles encargados del tratamiento que pudieran tener relación directa con el objeto de la reclamación.
- Copia del registro de actividades de tratamiento relativo a la mencionada actividad, con los datos exigidos por el artículo 30 RGPD y su base legal.
- A la vista de la situación reclamada, detalle de las medidas de seguridad técnicas y organizativas (aplicables tanto a los sistemas automatizados como al papel) ya implementadas por el responsable, así como de las medidas adoptadas para solucionar la incidencia objeto de la reclamación y las adoptadas para evitar que se produzcan



incidencias similares en el futuro. En especial, las medidas que garanticen la confidencialidad de la documentación que contenga datos de carácter personal, evitando el posible acceso a los mismos por parte de terceros.

- Documentación acreditativa sobre la existencia de protocolos, normas, procedimientos o reglas que puedan existir en el mencionado Ayuntamiento sobre el tratamiento de atestados policiales como el que da origen a la reclamación.
- Cualquier otra información relevante o actuación llevada a cabo en relación con los hechos reclamados; en particular, cualquier respuesta que haya podido dirigirse a la persona reclamante, con la acreditación de su remisión, y en su caso, recepción.

En contestación al requerimiento anterior, el 11 de julio de 2021 este Consejo recibió informe del DPD donde se señalaba que:

“Que cabe archivar la causa del presente expediente habida cuenta del archivo de diligencias que la Fiscalía de Área de Jerez ha realizado con respecto la filtración de datos del atestado que la Policía Local pudo realizar en aras de la tramitación del atestado y hoy reclamante, *[el reclamante]*, en virtud del incidente de tráfico acaecido en *[aaaa]*.

Que la Fiscalía tomó dicha decisión ante la imposibilidad de probar quien pudo haber realizado dicha comunicación de datos.

Que, por parte del Ayuntamiento de Jerez se tomaron las diligencias oportunas para poder indagar, sin éxito, sobre el origen de la filtración a través de la ayuda del área de informática: para ello se revisó el control de accesos a la información contenida en la unidad de red de la Policía verificando que exclusivamente el personal de Policía tiene acceso a dicha información mediante la comprobación de permisos. No obstante, se informó a este Consejo (en informe del Intendente de Policía) de la imposibilidad de poder asegurar al cien por cien aún bajo las medidas adoptadas por este Ayuntamiento y el control de autorizaciones que ‘siempre es posible sacar una o varias “fotos” de la pantalla que se está visualizando, sin que esto llegue a dejar rastro’.

Que, entre las medidas adoptadas por este Ayuntamiento, previamente comunicadas a este Consejo por medio del mencionado informe se encontraba el recordatorio de la obligación del personal de Policía a mantener el secreto profesional”.



Se adjuntaba copia del registro de actividades de tratamiento relativo a la actividad de tratamiento "Policía local" responsabilidad del órgano reclamado.

Quinto. Tras haberse elaborado el informe correspondiente a las actuaciones previas de investigación, el 23 de septiembre de 2021 el director del Consejo dictó Acuerdo de Inicio de procedimiento sancionador contra el Ayuntamiento de Jerez de la Frontera, con NIF P1102000E, por la presunta infracción del artículo 32.1 RGPD, tipificada en el artículo 83.4 RGPD y sancionable con apercibimiento de acuerdo con el artículo 77.2 LOPDGDD.

Sexto. Notificado el acuerdo de inicio al órgano reclamado, este, el 6 de octubre de 2021, presentó escrito de alegaciones, en el que, en síntesis, manifestaba lo siguiente:

"En reiterarnos en que cabe archivar la causa del presente expediente habida cuenta del archivo de diligencias que la Fiscalía de Área de Jerez ha realizado con respecto a la filtración de datos del atestado que la Policía Local pudo realizar en aras de la tramitación del atestado y hoy reclamante, *[el reclamante]*, en virtud del incidente de tráfico acaecido en *[aaaa]*.

Que la Fiscalía tomo dicha decisión ante la imposibilidad de probar quien pudo haber realizado dicha comunicación de datos.

Que, el área de informática del Ayuntamiento realizó las tareas y diligencias oportunas para poder indagar sobre el posible origen de la filtración comprobándose, finalmente, que no había registro de haber sucedido extracción alguna de las imágenes de los sistemas informáticos del Ayuntamiento.

Que, no obstante, lo anterior las imágenes objeto de la presente reclamación, pudieron ser obtenidas por medios analógicos, muy probablemente mediante fotografía tomada de los documentos a través de teléfono móvil o cámara tal y como se sustrae de la imagen facilitada por los medios de prensa, en la que consta claramente los sellos de goma o tampones y las firmas manuscritas de los intervinientes [...]."

Séptimo. Finalizada la instrucción del procedimiento, se procedió a realizar la correspondiente propuesta de resolución, que fue notificada al presunto infractor el 15 de marzo de 2022, estableciendo el plazo de diez días para la formulación de alegaciones, de conformidad con el



artículo 89.2 LPACAP y en relación con el artículo 73.1 de la misma norma.

Con fecha 28 de marzo de 2022 se recibe en el Consejo las alegaciones del órgano incoado al procedimiento sancionador, en las que se indica:

“PRIMERA. - Que, en relación al Fundamento de Derecho Tercero de la Propuesta de Resolución de Procedimiento Sancionador, no existe prueba que permita acreditar la filtración de la información a los medios de comunicación o a cualquier tercero no autorizado por parte de un empleado municipal; no hay forma posible de probar que las imágenes hubiesen sido obtenidas por el personal del Ayuntamiento, ni eliminar la posibilidad de que estas hubiesen sido obtenidas por el mismo interesado, su abogado o allegados.

Debemos tener en cuenta que, en el procedimiento sancionador, se debe probar los hechos constituyentes de infracción, y que en el presente caso no hay forma de probarlo. La actividad probatoria es esencial para garantizar el derecho fundamental a la presunción de inocencia, reconocido en el artículo 24.2 de la Constitución Española. La sentencia STS de 3 de junio de 2008 (rec. 146/04), que hace referencia a la doctrina del Tribunal Constitucional que señala que *“el principio de presunción de inocencia garantiza el derecho a no sufrir sanción que no tenga fundamento en una previa actividad probatoria”*, se reitera en otras como la STS 33/2000, de 14 de febrero.

Del mismo modo, debemos hacer referencia al principio de presunción de veracidad, derecho que ostentan las personas dotadas de autoridad pública en el desempeño de sus funciones, por lo que su palabra prevalece sobre la del no funcionario. Regulado en el artículo 77.5 de la Ley 39/2015, de 1 de octubre, Procedimiento Administrativo Común de las Administraciones Públicas, así como en el artículo 52 de la Ley Orgánica 4/2015, de 30 de marzo de protección de la seguridad ciudadana. Se trata de un principio *iuris tantum*, por lo que admite prueba en contrario; del mismo modo no se ha probado ni se puede probar la no veracidad de los empleados públicos participantes en el procedimiento referente al presente caso.

SEGUNDA.- Que, relativo al Fundamento de Derecho Cuarto, y de conformidad a la doctrina del Tribunal Supremo (la recientísima Sentencia de 15 de febrero de 2022 que comentamos ayer y que también te adjunto) *“la obligación que recae sobre el responsable*





del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas.” Señalando que, “tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado.”

Que, por parte del Ayuntamiento de Jerez se tomaron las medidas de seguridad, tanto por la Policía Local, así como el Departamento de informática, entre otras, se encontraba el recordatorio de la obligación del personal de Policía a mantener el secreto profesional.

Del mismo modo en el artículo 32.4 del RGPD, se indica que el Ayuntamiento en este caso, tomará las “medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros”. Por lo que, consecuentemente, nos encontramos ante una obligación de resultado, y no de medios, las obligaciones derivadas de la legislación se han realizado por parte del Ayuntamiento, por lo que, y de conformidad a la doctrina del Tribunal Supremo, no es exigible la infalibilidad de las medidas adoptadas.

TERCERA.- Que, las medidas que se describen en el artículo 32.1 del RGPD, se tratan de medidas genéricas, y que en relación a estas, los empleados del Ayuntamiento, encargados de tramitar el relativo expedientes, realizaron sus funciones de manera profesional y como se indica en el protocolo; y que de conformidad a las indagaciones y los informes realizados por el departamento de informática y de policía, no había incidencias detectadas. Recordamos que, entre las múltiples posibilidades, la información puede haberse filtrado mediante medios analógicos, carecientes de medidas de seguridad para evitarlo.

[...]”

Octavo. Es importante destacar que los plazos aplicables a las distintas fases del procedimiento de



resolución de la reclamación se han visto afectados por lo establecido en el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 o, en su caso, en las prórrogas del mismo.

HECHOS PROBADOS

De los documentos obrantes en el expediente y de las actuaciones practicadas, pueden considerarse como hechos probados los siguientes:

Primero. Una copia del atestado, o parte del mismo, levantado por agentes de la policía local el [dd/mm/aa] y bajo custodia en las dependencias policiales (Inspección de Guardia) terminó siendo objeto de publicación en medios de comunicación con los datos personales que contenían (Diligencias n.º [nnnnn]), extremo reconocido en los informes municipales: *"...aparecía publicado en el periódico [nombre del medio de comunicación] fotos del atestado relativo a la [persona] en cuestión...la aparición de parte del atestado en algunos medios de comunicación..."*.

Segundo. El órgano reclamado no pudo dar explicación alguna a la ruptura de la cadena de custodia del documento público ni constatar la verificación de las medidas de seguridad implantadas que hubiesen impedido dicha filtración a terceros.

Por un lado, se menciona que la documentación pasa de agentes de un turno a otro con cambios físicos de la misma; concretamente en el turno de noche el día [dd/mm/aa] el atestado se guardó en una taquilla personal de la Inspección de Guardia, y por otro se indica por la corporación local que no existen implantados sistemas de seguridad que permitan averiguar la trazabilidad del fichero en cuestión, y que los sistemas informáticos pueden estar expuestos a posibles escaneados o fotografías de los mismos.

FUNDAMENTOS DE DERECHO

Primero. La competencia para resolver el procedimiento sancionador por posible



incumplimiento de la normativa de protección de datos personales, en relación con los hechos descritos, corresponde al director del Consejo en virtud de lo establecido en los artículos 43.1 y 48.1.i) de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (en adelante, LTPA), en los artículos 10.3.b) y 10.3.i) de los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía (aprobado por Decreto 434/2015, de 29 de septiembre) y en los artículos 57 y 64.2 LOPDGDD.

El Consejo, como autoridad autonómica de protección de datos personales, y dentro de su ámbito competencial, ejerce las funciones y potestades establecidas en los artículos 57 y 58 RGPD.

Segundo.- El artículo 32 RGPD se refiere a la "seguridad del tratamiento", y en su apartado primero establece que:

"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".*

Tercero. De acuerdo con la documentación obrante en el expediente, y en relación con los hechos probados expresados anteriormente, ha quedado acreditado que una copia del atestado, o parte del mismo, levantado por agentes de la policía local el [dd/mm/aa] y bajo custodia en las dependencias policiales terminó siendo objeto de publicación en medios de comunicación con los datos personales que contenían.



Notificado el acuerdo de inicio al órgano reclamado y como se indica en los Antecedentes, este presentó escrito de alegaciones, el 6 de octubre de 2021, donde, entre otras cuestiones, indicaba “que no hay manera de probar si las imágenes pudieron ser obtenidas por personal del Ayuntamiento, así como podrían haber sido obtenidas por el mismo interesado, el abogado del interesado o allegados del mismo interesado”.

Sin embargo, el órgano reclamado no pudo dar explicación alguna a este organismo sobre la ruptura de la cadena de custodia del documento público ni constatar la verificación de las medidas de seguridad implantadas que hubiesen impedido dicha filtración a terceros.

Por consiguiente, de acuerdo con todo lo expuesto, se entiende que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente del órgano reclamado.

Cuarto.- Notificada la propuesta de resolución al órgano reclamado y como se indica en los Antecedentes, este presentó escrito de alegaciones, el 28 de marzo de 2022.

En las mismas se reitera que no existe prueba que permita acreditar la filtración de la información a los medios de comunicación o a cualquier tercero no autorizado por parte de un empleado municipal; que no hay forma posible de probar que las imágenes hubiesen sido obtenidas por el personal del Ayuntamiento y que estas podrían haber sido obtenidas por el mismo interesado, su abogado o allegados. Sin embargo, el Consejo no se pronuncia sobre el origen de la filtración y divulgación de los datos personales del reclamante. Lo que se analiza es si las medidas técnicas y organizativas implantadas en el ayuntamiento eran apropiadas para garantizar una seguridad adecuada de los datos personales que se tratan, de manera que impida el quebrantamiento del principio de confidencialidad y el órgano reclamado no ha podido constatar la adecuación de las medidas de seguridad implantadas a los efectos de que fueran suficiente para minimizar el riesgo de filtración de datos personales a terceros.

Además, como ya se ha mencionado, una copia del atestado, o parte del mismo, levantado por agentes de la policía local y bajo custodia en las dependencias policiales (Inspección de Guardia) terminó siendo objeto de publicación en medios de comunicación.



Defiende también el órgano reclamado que *"la obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas."* Afirmación esta que no cuestiona este Consejo, ya que, como ya se ha mencionado, el análisis abordado se centra en la existencia o no de dichas medidas, cuya aplicación, a fecha de la presente resolución, no ha quedado acreditada.

Por lo tanto, de acuerdo con todo lo expuesto, se entiende que las alegaciones presentadas a esta propuesta no desvirtúan el contenido esencial de la infracción que se declara cometida, ni suponen causa de justificación o exculpación suficiente del órgano reclamado que, como responsable del tratamiento, incumplió, por las circunstancias expuestas anteriormente, el mencionado artículo 32.1 RGPD en relación con la falta de aplicación de medidas técnicas y organizativas apropiadas para garantizar la confidencialidad a la hora de custodiar los datos personales del reclamante, pudiendo dar lugar a una filtración de los mismos a los medios de comunicación entre los días [dd y dd/mm/aa].

Quinto. El incumplimiento de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43"* del RGPD se contempla tipificada como infracción a la normativa de protección de datos personales en el artículo 83.4 RGPD; los hechos atribuibles al órgano reclamado están igualmente considerados, a efectos de prescripción, como infracción grave en el artículo 73.f) LOPDGDD:

"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 RGPD transcrito.

Sexto. El artículo 58.2 RGPD dispone que:

"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:



[...]

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

[...]

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;

[...]”.

Por otra parte, el artículo 77 LOPDGDD establece el régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento; en particular, en su apartado 1.d) incluye a “[/]os organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas”. En el mencionado artículo, en su apartado 2, se señala que:

“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”.

Así, de acuerdo con el artículo 77.2 LOPDGDD, la sanción que procede imponer al responsable del tratamiento es el apercibimiento.

Se considera además que el responsable del tratamiento ha de aplicar las adecuadas medidas organizativas y técnicas de seguridad en relación con el tratamiento, de modo que se minimice el riesgo de posibles filtraciones de datos. A estos efectos, y de acuerdo con la Disposición adicional primera de la LOPDGDD, las medidas mínimas a aplicar serán las previstas en el Esquema Nacional de Seguridad (ENS). Dicho ENS ha sido recientemente actualizado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Séptimo. En relación con la notificación de la resolución del procedimiento sancionador, el artículo 77.2 LOPDGDD dispone que “[/]a 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".

Además, el artículo 77.4 LOPDGDD señala que "[s]e 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", y el 77.56 LOPDGDD, que "[s]e 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".

En virtud de todo lo expuesto y de acuerdo con la legislación aplicable, el Director del Consejo de Transparencia y Protección de Datos de Andalucía

RESUELVE

Primero. Dirigir un APERCIBIMIENTO al Ayuntamiento de Jerez de la Frontera, con CIF P1102000E, por infracción del artículo 32.1 RGPD, tipificada en el artículo 83.4 RGPD.

Segundo. Como medida adicional, se insta al mencionado Ayuntamiento a la aplicación de las adecuadas medidas técnicas y organizativas para mejorar la seguridad del tratamiento; al menos han de implantarse las medidas que se contemplan en el Esquema Nacional de Seguridad para las características del tratamiento objeto de la resolución. El Ayuntamiento deberá comunicar en el plazo de un mes desde la notificación de la misma las actuaciones realizadas al respecto.

Tercero. Que se notifique la presente resolución al órgano incoado.

Cuarto. Que se comunique la presente resolución al Defensor del Pueblo Andaluz, de conformidad con lo establecido en el artículo 77.5 LOPDGDD.

En consonancia con lo establecido en el artículo 50 LOPDGDD, la presente Resolución se hará pública, disociando los datos que corresponda, una vez haya sido notificada a los interesados.



Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer recurso potestativo de reposición ante este Consejo, en el plazo de un mes, o interponer directamente recurso contencioso-administrativo ante el Juzgado de lo Contencioso Administrativo de Sevilla que por turno corresponda, en el plazo de dos meses, en ambos casos a contar desde el día siguiente al de su notificación, de conformidad con lo dispuesto en los artículos 30.4, 123 y 124 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en los artículos 8.3 y 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Conforme a lo previsto en el art. 90.3.a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta ante este Consejo su intención de interponer recurso contencioso-administrativo y traslada al mismo, una vez interpuesto, la documentación que acredite su presentación. Si el Consejo no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo correspondiente o en dicho recurso no se solicitara la suspensión cautelar de la resolución, se daría por finalizada la mencionada suspensión.

**EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS DE ANDALUCÍA**

Jesús Jiménez López

