- **Expediente N.º: PS/00596/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 7 de enero de 2021, D. ***A.A.A.*** (en adelante, la parte reclamante), interpuso reclamación ante la Agencia Española de Protección de Datos contra el AYUNTAMIENTO DE OURENSE, con NIF P3205500F (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

En fecha día 5 de enero, sobre las 22h, en Ourense, en la calle ******DIRECCIÓN.1***, el Agente ***nº***AGENTE.1*** de la Policía Local, le solicitó el DNI para su identificación. En el momento de tenerlo en su mano, lo fotografió sin su consentimiento y sin aclararle el uso que iba a hacer de dichos datos. Debido a esta situación de indefensión y al dispositivo utilizado por el Agente, considera que no tiene garantizada la seguridad de sus datos personales y fotografía del DNI, por lo que solicita que dicha imagen sea eliminada, al no tener dicho Agente motivos para su uso y almacenamiento.

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), mediante notificación electrónica, fue recibido en fecha 1 de marzo de 2021, como consta en el certificado que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: En fecha 12 de mayo de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

En fecha 26 de mayo de 2021, se requirió por la Inspección de Datos, al Ayuntamiento de Ourense, para que, en el plazo de diez días, aportara determinada información y documentación con objeto de aclarar los hechos denunciados.

En fecha 7 de julio de 2021, tuvo entrada un escrito de respuesta a dicho requerimiento en el que, en síntesis, se pone de manifiesto lo siguiente:

Respecto a la licitud del tratamiento de datos personales por parte de la Policía Local a la hora de requerir los datos de un ciudadano y que lo hagan mediante la realización de una fotografía a su Documento Nacional de Identidad:

Exponen que el Reglamento General de Protección de Datos (RGPD) diseña un sistema de legitimación basado en seis bases jurídicas que no mantienen entre sí ninguna relación de prioridad o prelación.

En particular, y para el ámbito de la Administración Local, son relevantes las siguientes:

- El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En el presente caso alegan lo siguiente:

- Las Fuerzas y Cuerpos de Seguridad del Estado se encuentran totalmente autorizados para solicitar o tomar los datos de las personas con motivos de investigación, preventivos o para aquellos casos que se produzcan en el contexto de que el individuo pueda estar incurriendo en algún tipo de ilegalidad o infracción de la ley, todo ello de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, la Directiva Europea 2016/680, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y el Reglamento General de Protección de Datos, de misma fecha.

- La Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, establece en los artículos 16.1 y 9.2 que los ciudadanos deben obligatoriamente presentar sus datos personales o DNI cuando los agentes de las Fuerzas y Cuerpos de Seguridad les requieran la identificación en las siguientes situaciones:

  a) Cuando existan indicios de que han podido participar en la comisión de una infracción.

  b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito.

- En el momento en el que un agente de la autoridad realice fotografías de un documento de identidad, es necesario situar en contexto legal dicho

procedimiento, teniendo en cuenta que se debe cumplir la normativa impuesta para aquellos que se ocupan del tratamiento de los datos personales de un individuo. Así, en la Ley Orgánica 3/2018 que se ocupa de las Garantías de Derechos Digitales y de la Protección de Datos Personales se establece que el agente que lleve a cabo el tratamiento de la información personal de ciudadanos debe garantizar que dicho procedimiento cumpla con las medidas de confidencialidad y seguridad establecidas para la protección de datos e información personal. Por tanto, de acuerdo con lo anterior, los Agentes de las FyCSE entienden que podrán tratar datos personales cuando lo soliciten a efectos de identificación. Con todo, cuando un agente toma una fotografía del DNI, debemos poner el foco dentro del ámbito del cumplimiento de las medidas de seguridad que la normativa de protección de datos exige al responsable del tratamiento.

- La LO 3/2018 de Protección de Datos personales y Garantía de derechos digitales, exige a los responsables del tratamiento la adopción de las correspondientes medidas de seguridad de índole técnica y organizativa necesarias que garanticen que el tratamiento es conforme a la normativa vigente. Es decir, la toma de los datos de filiación de un ciudadano para su posterior tratamiento debe realizarse con métodos que garanticen la seguridad y confidencialidad de los datos personales. En el caso de que los agentes utilicen dispositivos particulares para la toma de imágenes de los datos personales que contiene el DNI en el ejercicio de sus funciones no garantiza totalmente la seguridad de los datos, ya que el uso privado de que cada agente pueda hacer de su dispositivo no resultaría compatible con las medidas de seguridad que para el ejercicio de las funciones de indagación, investigación y prevención de delitos e infracciones deban adoptarse. Además, conviene señalar que dicho dispositivo queda fuera del control del responsable del tratamiento.

- Cuestión distinta será si el dispositivo a través del cual se toma la imagen pertenece a la organización, en lugar de ser personal, es corporativo, siendo susceptible de que se le puedan aplicar las políticas y medidas de control y seguridad que garanticen que dicho tratamiento se realiza conforme a la normativa de protección de datos.

En relación con la reclamación presentada por el reclamante en la que manifiesta que un Agente de la Policía Local le solicitó la identificación y le fotografió con un móvil sin su consentimiento el DNI, por lo que solicita la supresión de las imágenes tomadas, manifiestan:

- Manifiestan que el ayuntamiento ha revisado procedimientos llevados a cabo por la Jefatura de Policía a los efectos de conocer el alcance y procedimientos de uso de dispositivos móviles.

- ***(…).***

- Desde la Jefatura de Policía se ha elaborado un manual de uso para la incorporación de imágenes a los expedientes. En la formación se insistió en que todas las fotografías se tienen que tomar con el terminal de dotación, quedando pendiente y en elaboración instrucción oficial de uso adecuado.

- Alegan que se considera ajustado a derecho y a la normativa en vigor en materia de tratamiento y protección de datos personales el uso de

dispositivos corporativos por parte de la Policía Local de Orense con y para la finalidad descrita.

Respecto a la solicitud de eliminación de la imagen del DNI tomada por el agente:

- En cuanto al tratamiento de las fotografías tomadas, manifiestan que estas serán eliminadas una vez concluya la finalidad para la cual fueron tomadas, es decir, apertura de expediente, el cual a fecha de hoy se encuentra todavía en trámite.

- Manifiestan que toda vez que el expediente sigue en curso, se le notifica a ***D. A.A.A.*** la circunstancia en la que se encuentra su tratamiento de datos personales.

Respecto a la información facilitada al reclamante relativa al tratamientos de los datos de carácter personal recabados:

- No consta que se haya facilitado información al reclamante en los términos previstos en el art. 13 del RGPD.

Con fecha 9 de septiembre de 2021, se solicitó por la Inspección de Datos al Ayuntamiento de Orense información y documentación con objeto de aclarar el contexto legal y el ámbito (penal o administrativo) en los que se enmarca la actuación del Agente de Policía.

Con fecha 18 de octubre de 2021, tuvo entrada escrito de respuesta al requerimiento en el que ponen de manifiesto que, en el caso que nos ocupa, se trata de un acta de denuncia por saltarse el toque de queda establecido por la situación de pandemia y adjuntan una captura de pantalla, en la que consta el inicio del expediente sancionador en la Subdelegación, la cual les informó que lo derivaran a la Xunta ya que era la competente para sancionar estos temas.

Con fecha 26 de octubre de 2021, se solicitó por la Inspección de Datos al Ayuntamiento de Orense, en relación con la fotografía tomada por la Policía Local del documento de identidad de ***A.A.A.***, aclaración sobre si dicha fotografía fue tomada con un terminal móvil corporativo, o se hizo uso de otro dispositivo ajeno al Ayuntamiento.

Con fecha 25 de noviembre de 2021, tuvo entrada escrito de respuesta al requerimiento en el que ponen de manifiesto lo siguiente:

- La fotografía fue tomada por un dispositivo distinto a los corporativos.

- Desde el 16 de marzo de 2021, la Policía Local del Ourense utiliza en sus actuaciones, dispositivos corporativos.

- Desde la Jefatura de Policía se ha elaborado un manual de uso para la incorporación de imágenes a los expedientes.

- En cuanto a la fotografía obtenida, ésta fue eliminada del dispositivo una vez que concluyó la finalidad para la que fue tomada.

QUINTO: En fecha 5 de abril 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.c) 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 5 de abril de 2022, como consta en el certificado que obra en el expediente.

SEXTO: Transcurrido el plazo otorgado para la formulación de alegaciones al acuerdo de inicio del procedimiento, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP) -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

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 7 de enero de 2021, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, toda vez que un Agente de la Policía Local fotografió su DNI para su identificación, sin su consentimiento.

SEGUNDO: La fotografía fue tomada por un dispositivo distinto a los corporativos de la Policía Local.

TERCERO: La fotografía fue realizada en el contexto de la identificación del reclamante en la constatación de una posible infracción como saltarse el toque de queda establecido por la situación de pandemia.

CUARTO: En relación con el tratamiento de la fotografía del DNI, el reclamado afirma que será eliminada “una vez concluya la finalidad para la cual fueron tomadas, es decir, apertura de expediente”, el cual, a fecha de formulación de esa alegación, se encontraba todavía en trámite.

FUNDAMENTOS DE DERECHO

PRIMERO: 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*."

SEGUNDO: Según se establece en el apartado III del "Preámbulo" de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC), *"(…) se habilita a las autoridades competentes para acordar distintas actuaciones dirigidas al mantenimiento y, en su caso, al restablecimiento de la tranquilidad ciudadana en supuestos de inseguridad pública, regulando con precisión los presupuestos, los fines y los requisitos para realizar estas diligencias, de acuerdo con los principios, entre otros, de proporcionalidad, injerencia mínima y no discriminación (…)".*

Y así se establecen en los artículos 9.2 y 16.1 de la LOPSC, respecto de la obligación de exhibir y permitir la comprobación del DNI por parte de los agentes de las Fuerzas y Cuerpos de Seguridad del Estado.

En el artículo 9, sobre las obligaciones y derechos del titular del Documento Nacional de Identidad, indica que:

"2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo y permitir la comprobación de las medidas de seguridad a las que se refiere el apartado 2 del artículo 8 cuando fueren requeridas para ello por la autoridad o sus agentes, para el cumplimiento de los fines previstos en el apartado 1 del artículo 16. De su sustracción o extravío deberá darse cuenta tan pronto como sea posible a la comisaría de Policía o puesto de las Fuerzas y Cuerpos de Seguridad más próximo".

En su artículo 16, sobre la Identificación de las personas, se establece que:

1. En el cumplimiento de sus funciones de indagación y prevención delictiva, así como para la sanción de infracciones penales y administrativas, los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas en los siguientes supuestos:

a) Cuando existan indicios de que han podido participar en la comisión de una infracción.

b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito. En estos supuestos, los agentes podrán realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados.

En la práctica de la identificación se respetarán estrictamente los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social.

Por tanto, las Fuerzas y Cuerpos de Seguridad del Estado pueden tratar los datos personales de los ciudadanos para la prevención, investigación, detección o enjuiciamiento de infracciones penales y para el desempeño de las funciones de interés público que les son propias. No obstante, estos tratamientos deben ser realizados respetando en todo momento, lo establecido en la normativa vigente en materia de protección de datos de carácter personal, el RGPD y la LOPDGDD, respectivamente.

TERCERO: En lo que respecta a la aplicación de la normativa de protección de datos al supuesto planteado, debe tenerse en cuenta que el RGPD, en su artículo 32, exige a los responsables del tratamiento, la adopción de las correspondientes medidas de seguridad necesarias que garanticen que el tratamiento es conforme a la normativa vigente, así como garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, solo los pueda tratar siguiendo instrucciones del responsable.

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).

Por otra parte, el Considerando (74), del RGPD indica que: *"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."

Así, la toma de los datos personales de identificación de un ciudadano, por parte de los agentes de la Policía, debe realizarse con métodos que garanticen la seguridad y confidencialidad de estos, siguiendo las instrucciones del responsable del tratamiento.

En el presente caso, el reclamante denuncia que cuando mostró el DNI, el Agente realizó una fotografía del documento con un móvil, extralimitándose con ello en los derechos que le asisten, mientras que, por su parte, la parte reclamada manifiesta que la fotografía fue tomada con un dispositivo distinto a los corporativos.

Por tanto, debe examinarse si tales cámaras domésticas y teléfonos móviles pueden garantizar la seguridad de los datos de forma que no se produzcan pérdidas o alteraciones de los datos y, muy especialmente, dada la generalización de uso de dispositivos inteligentes, la posibilidad de acceso por terceros a los datos en ellas almacenados. Debe así tenerse en cuenta que puede producirse inadvertidamente una cesión de datos a terceros.

Teniendo en cuenta los riesgos señalados debe considerarse que el uso de cámaras o móviles personales de los agentes no garantiza la seguridad de los datos, en tanto que los usos privados que cada agente pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de seguridad que para el ejercicio de las funciones de policía deben adoptarse por los responsables del fichero policial del que formarán parte tales grabaciones.

Asimismo, en el caso de que se utilizasen dispositivos inteligentes que se hayan entregado con carácter oficial para su uso con fines policiales, éstos deberán responder a las exigencias normativas, debiendo, en particular, adoptarse todas las precauciones para impedir accesos indebidos a los datos que con ellos se capten.

En el caso concreto que se examina, la actuación realizada a través del teléfono móvil distinto a los corporativos para la toma de datos del reclamante constituye infracción a lo dispuesto en el artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

Establece el artículo 83.4.a) del citado RGPD 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.

CUARTO: En el artículo 5 del RGPD, se establecen los principios relativos al tratamiento de los datos personales por el responsable y/o encargado de los mismos y en su apartado 1.c) se especifica que: *"los datos personales serán: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»).*

Hay que aclarar que este artículo no limita el exceso de datos, sino la necesidad. Es decir, los datos personales serán, "*adecuados, pertinentes y limitados a la necesidad*", para la que fueron recabados, de tal manera que se debe evaluar si el objetivo perseguido podría haberse alcanzado por otro medio, sin realizar un tratamiento excesivo de datos, como en nuestro caso. Así lo establece también el Considerando 39 del RGPD, cuando indica que: *"Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios."*

Por tanto, únicamente se tratarán los datos que sean, adecuados, pertinentes y no excesivos en relación con el fin para el que se obtienen o tratan. Las categorías de datos seleccionados para su tratamiento deben ser los estrictamente necesarios para lograr el objetivo declarado y el responsable del tratamiento debe limitar estrictamente la recogida de datos a aquella información que esté directamente relacionada con el fin específico que se intenta alcanzar.

En el supuesto examinado el tratamiento ha consistido en la realización de la fotografía de DNI a través del móvil personal del policía, así como su conservación, hasta la apertura del expediente administrativo. Este tratamiento es claramente excesivo, debiendo destacar que el principio de "minimización de datos" impone además la supresión de la imagen inmediatamente después de que se ha producido la mencionada identificación.

A estos efectos, es preciso señalar que la finalidad alegada por el reclamado para el mantenimiento de la fotografía sería el "volcado en la aplicación para la apertura del expediente". Es decir, ni siquiera se alega una presunta finalidad de incluir el documento en el propio expediente, que en todo caso debería ser motivada. Con ello, carece aún de menor justificación la conservación de la imagen, que se encuentra desprovista de ninguna finalidad.

Por todo ello, la actuación en este supuesto del reclamado supone la vulneración del principio de "minimización de datos", recogido en el citado artículo 5.1.c) RGPD, donde se establece que el tratamiento de los datos personales debe ser *"adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados",* tipificado en el artículo 83.5 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.

QUINTO: 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 constituye el elemento de la culpabilidad.

SEXTO: El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

"*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.c) del RGPD, al realizar un tratamiento excesivo de los datos personales con relación a la finalidad para la se estaba recabando, y por la infracción del artículo 32 del RGPD, al considerar que la realización de la fotografía del DNI del reclamante con un teléfono móvil no corporativo es un acto que no garantiza un nivel de seguridad adecuado al riesgo del tratamiento de los datos personales.

SÉPTIMO: 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.c) 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 OURENSE, con NIF P3205500F, por una infracción del artículo 5.1.c) del RGPD, tipificada en el artículo 83.5 del RGPD.

SEGUNDO: SANCIONAR con APERCIBIMIENTO al AYUNTAMIENTO DE OURENSE, con NIF P3205500F, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

TERCERO: REQUERIR al AYUNTAMIENTO DE OURENSE, 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 al AYUNTAMIENTO DE OURENSE.

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.

938-100322

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