- **Procedimiento Nº: PS/00420/2018**

938-051119

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 6/09/2018 se recibe reclamación de ***A.A.A.*** en nombre de ***B.B.B.*** (en lo sucesivo el reclamante), que trabaja como policía local en ******LOCALIDAD.1***, contra el AYUNTAMIENTO DE ***LOCALIDAD.1 (POLICÍA LOCAL) (en lo sucesivo reclamada).

Manifiesta que desde la plataforma digital de su puesto de trabajo, se tiene acceso por parte de todos los agentes a todos los datos de los informes tanto de trabajo como de cualquier carácter personal y de salud. Sin usar ningún tipo de filtro, se pueden visionar los datos personales de otros funcionarios, dirección, datos médicos, estado civil. Aunque no se pueden modificar, si se accede en modo lectura, y no queda constancia de quien accede.

Indica que en la plataforma figura un informe en el que se revelan sus datos médicos por parte de un superior a otro, siendo el informe perfectamente visible por cualquier compañero.

Aporta copia de la impresión de una pantalla obtenida desde la plataforma, "*en el puesto de trabajo de otro compañero*" para "*acreditar la facilidad con que cualquiera accede a los datos*", y se comunican sus datos personales entre dos superiores, datos a los que puede acceder cualquier compañero, sin dejar rastro.

En la pantalla se contiene un informe con el título "*Régimen interior novedades*" ejercicios de tiro no realizados por el PL ***XXX***-jefe de turno con un número y nombre y apellidos y en Agentes dos números.

En el comentario se narran los hechos de un ejercicio de tiro que el policía ***XXX*** no pudo realizar aludiendo que tenía la tensión alta y que aportaría un informe médico. Constando que se entrevistó con el policía para averiguar si es una cuestión duradera o transitoria y exponiéndose los motivos y la falta de ánimo del policía.

SEGUNDO**:** A la vista de los hechos manifestados en la reclamación se trasladó a la reclamada para que informara:

1. Especificación clara de las causas que han motivado la incidencia que ha dado lugar a la reclamación.

2. Detalle de las medidas adoptadas por el responsable para solucionar la incidencia y para evitar que se produzcan nuevas incidencias como la expuesta.

3. Documentación acreditativa de que se ha atendido el derecho del reclamante a ser informado sobre el curso y el resultado de la presente reclamación.

Se constata que el 15/10/2018 la reclamada recibe el escrito, y con fecha 26/11/2018, se recibe respuesta, indicando que se han remitido al reclamante los dos informes que se acompañan en un escrito de 19/11/2018.

a) El primero, firmado por un Inspector Jefe, de 2/11/2018, indica sobre la reclamación que "*La base de datos a que hace alusión el reclamante es una base de carácter interno, a la cual solo se puede acceder haciendo con usuario y contraseña, acreditándose que el acceso solo se hace por componentes policiales, los cuales tienen el deber de sigilo, guardar secreto profesional*". Distingue entre tratamientos con fines administrativos de los de investigación policial. Añade la obligación de observar por los funcionarios el sigilo sobre los asuntos que conozcan y manifiesta solo accedieron a la base de datos componentes policiales, concluyendo que no ha existido revelación de secretos, falta de sigilo profesional o violación del secreto, y que no se precisa ninguna toma de medidas considerando que los datos están protegidos.

El segundo, del Servicio de Telecomunicaciones e informatica, de 30/10/2018, indica que el acceso al directorio activo se efectúa con usuario y contraseña. "*La aplicación "informes y atestados de Policía Local fue desarrollada por la plana mayor y el servicio de informatica del Ayuntamiento*". Su finalidad es recoger todas las actuaciones efectuadas por los agentes de la jefatura con indicación entre otros de cumplimentación del campo "*informe*" que es de libre redacción por cada agente redactor. Una vez completado, se incluye en un circuito de supervisiones que comienzan en el jefe de turno y termina con la supervisión de la plana mayor y su posterior archivo. Indica que "todos los informes debían ser compartidos *de lectura para todos los agentes*".

En cuanto a la "*aplicación de Agentes*" se desarrolla como tabla auxiliar de otras tantas aplicaciones, con el fin de poder registrar los turnos de servicio, relación de agentes actuantes-informes y atestados, productividades realizadas, señalando que "*todos los agentes tienen acceso a los datos de la misma en igualdad de condiciones, en solo lectura sin que existan partes de la misma accesibles de forma restringida por la plana mayor*"

Se emite acuerdo de admisión a trámite de la reclamación el 4/12/2018.

TERCERO: Con fecha 6 y 7/02/2019 se reciben escritos del representante del reclamante indicando que se ha recibido escrito de la Policía Local, pero no del Delegado de Protección de Datos, y que la respuesta no se corresponde con "*los hechos denunciados*". Acompaña los escrito de la Policía, de 19/11/2018 en el que se indica que le acompañan informe del Inspector Jefe de 2/11/2018 y otro del responsable de implantaciones del Departamento de informática de 30/10/2018.

Con fecha 11/03/2019 se recibe escrito del reclamante indicando que no ha recibido comunicación de acuerdo tomado respecto de su reclamación.

CUARTO: Con fecha 12/07/2019, la Directora de la AEPD, inició un procedimiento de apercibimiento contra el AYUNTAMIENTO DE ***LOCALIDAD.1 (POLICÍA LOCAL) por presunta infracción del artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27/04/2016 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 (en lo sucesivo, RGPD), por una infracción que se recoge en el artículo 83.5.a) del RGPD, conforme señala el artículo 58.2.b) del RGPD en relación con el artículo 77.2 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

QUINTO: Con fecha 2/08/2019, la reclamada indica en sus alegaciones:

a) Informe emitido por el Inspector Jefe Accidental de Servicios Administrativos que en síntesis indica:

> -Se trasladó el acuerdo de inicio al área de informatica que comunica que "*se han llevado a cabo las medidas correctoras para evitar la incidencia a la que hace referencia el expediente, llevando a cabo la creación de una aplicación informática específica para la confección de informes personales y de régimen interior relativos a Agentes, garantizando la seguridad de los datos y su protección*."
>
> La aplicación queda restringida al Jefe de turno redactor del informe, el Agente sujeto pasivo del mismo, y el miembro de la plana mayor al que se destine el informe.
>
> Solo los mandos de la Jefatura pueden acceder a la aplicación para crear informes.
>
> Se informa a los Agentes que no utilicen la aplicación anterior "*informes y atestados*" para confección de escritos sobre régimen interior o informes personales.

b) Escrito del "*responsable de implantaciones del área de informatica*", de 29/07/2019 que señala lo mismo.

c) Reitera el envío del escrito de Inspector Jefe de policía local de 2/11/2018.

d) Aporta copia de un escrito dirigido al reclamante referencia ***YYYYY***-2018 de 8/11/2018 en el que figura que le remiten informes de 2/11/2018 y otro de Informatica de 30/10/2018.

SEXTO: Con fecha 10/02/2020 se emitió propuesta de resolución del literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione con apercibimiento al AYUNTAMIENTO DE ***LOCALIDAD.1 (POLICIA LOCAL), por una infracción del Artículo 5.1.f) del RGPD, de acuerdo con el artículo 83.5 del RGPD.*"

SÉPTIMO: Frente a la propuesta no se recibieron alegaciones.

HECHOS PROBADOS

1) El reclamante trabaja como Policía local en ******LOCALIDAD.1***. El desempeño de su puesto de trabajo se realiza en parte a través de una aplicación informatica. La aplicación permite introducir información y datos de las actuaciones profesionales de cada Agente.

2) El reclamante aporta copia impresa de la captura de una pantalla obtenida desde la plataforma informatica con la que trabaja, pestaña "*RÉGIMEN INTERNO*" en la que se lee: "*Régimen interior novedades*" "*ejercicios de tiro no realizados por el PL* ***XXX***" "*jefe de turno*" con su número y nombre y apellidos y en el campo "*Agentes*" dos números de agente, uno el del Jefe de turno. En el comentario se narran los hechos sucedidos "*con ocasión de las prácticas de tiro rutinarias que se vienen realizando por los componentes de la plantilla, el policía PL-****RRR*** *(instructor de tiro) me comunica que...*", se alude a las prácticas de tiro de las que formaba parte el policía reclamante que identifica por su número ***XXX.*** Se informa que lleva más de un año sin hacer las prácticas y "*siempre alega problemas médicos*" que "*me comunica que tenía la tensión alta y que aportaría un informe médico*". Se indica también que se entrevistó con el policía para averiguar si es una cuestión duradera o transitoria y exponiéndose los motivos y la falta de ánimo del policía.

3) La reclamada indica en alegaciones al acuerdo que ha variado el contenido de escritos de RÉGIMEN INTERNO, de modo que ha limitado los usuarios que pueden redactar, enviar y leer estos escritos. Se ha creado una aplicación específica para ello.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

En la STC 292/2000, de 30/11, queda delimitado el objeto y contenido del derecho a la protección de datos en los términos que se exponen a continuación.

El derecho fundamental a la protección de datos, consagrado en el artículo 18.4 de la Constitución Española, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, excluyendo del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, persigue garantizar a esa persona un poder de control sobre sus datos

personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

El derecho a la protección de datos tiene, por tanto, un objeto más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inseparablemente unidos al respeto de la dignidad personal, como el derecho al honor, y al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales - como aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo-, porque su objeto no es sólo la intimidad individual, protegida ya por el art. 18.1 CE , sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

Por lo que respecta a su contenido, el derecho fundamental a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. Entre ellos, destacan el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. De este modo se garantiza el poder de disposición sobre los datos personales

En el desarrollo de la prestación laboral, los funcionarios como cualquier otro empleado tienen derecho a la protección de sus datos, pues la relación estatutaria no excepciona la configuración de este derecho, ni puede considerarse como un título legitimador de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización (STC 99/1994).

En este caso, los comentarios habidos con ocasión de la celebración de un ejercicio de tiro del reclamante con su instructor, que contenían referencias a cuestiones de salud, psicológicas y del servicio no atañen a terceros, incluyendo entre estos sus compañeros, que aunque sean Policías y estén sometidos al deber de secreto, no por ello se puede negar que han podido conocer las circunstancias asociadas al reclamante, y cuya finalidad no era

esta.

Los hechos debieron haberse mantenido en la cadena de gestión ordinaria de asuntos entre las partes, sin que se hubiera dado posibilidad al acceso de los empleados, produciéndose una revelación de los hechos y una vulneración de su intimidad.

III

Se imputa a la reclamada la comisión de una infracción del artículo 5.1 f) del RGPD que señala:

"Los datos personales serán:

"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»).

El principio de seguridad de los datos impone la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar y garantizar que entre otros aspectos a título de ejemplo, no se produzca un "*acceso no autorizado*" por parte de terceros, o que terceros, no interesados, por la configuración de la aplicación como sucede en este caso puedan leer escritos referidos a la gestión interna de los asuntos de personal o régimen interno. La gestión del riesgo de que la información que va asociada a los datos personales no sea conocida por los no afectados o interesados ha fallado en el desarrollo de la aplicación informatica de la reclamada, que desde su diseño tiene que contar con salvaguardar dicho extremo para que no se vea vulnerada la confidencialidad de los mismos, sin que baste con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Además, todo responsable de un fichero debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica siendo responsable de que las mismas se cumplan y ejecuten con rigor, debiendo efectuar evaluaciones periódicas de su funcionamiento.

El RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales*" como "*todas aquellas violaciones de la seguridad que ocasionen 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*." Las incidencias de seguridad han de notificarse a la AEPD cuando constituya un riesgo para los derechos y libertades de las personas físicas, y en este caso se ha materializado ese riesgo con la disposición de los datos a terceros, aunque fueran del mismo colectivo y en el círculo de policías que manejan la base de datos y prestan servicios en la sede de la reclamada.

En el presente caso, se acredita la comisión de la infracción que se da al poder visualizar los empleados el contenido de informes internos que se tramitan en gestión de personal sobre obligaciones de los componentes policiales. En este sentido se debe incidir que si bien los accesos se lleven a cabo utilizando contraseña y usuario, no fue óbice para que por la configuración de los accesos, cada uno pudiera acceder libremente a este informe.

III

El artículo 83.7 del RGPD indica:

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

a) sancionar a todo responsable o encargado del tratamiento con 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;

El artículo 72.1.a) de la LOPDGDD indica: "*Infracciones consideradas muy graves*

"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".*

Añadiendo el artículo 77. 2 de la LOPGDD:

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."

En tal sentido, se cuenta con el cambio en la forma de gestionar los informes de régimen interior de los policías locales.

Por lo tanto, de acuerdo con la legislación aplicable,

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

PRIMERO: IMPONER una sanción de APERCIBIMIENTO al **AYUNTAMIENTO DE ***LOCALIDAD.1 (POLICIA LOCAL)**, con NIF ***P1103100B***, por una infracción del Artículo 5.1.f) del RGPD, de conformidad con el artículo 83.5 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución al **AYUNTAMIENTO DE ***LOCALIDAD.1 (POLICIA LOCAL)**.

TERCERO: COMUNICAR la presente resolución al DEFENSOR DEL PUEBLO, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

CUARTO: 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.

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