Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Identificación del expediente

Resolución de archivo de la información previa núm. IP 351/2018, referente al Ayuntamiento de (...).

Antecedentes

1. En fecha 14/12/2018, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una sección sindical por el que formulaba denuncia contra el Ayuntamiento de (...), con motivo de un presunto incumplimiento de la normativa sobre protección de datos de carácter personal.
La entidad denunciante exponía que el Ayuntamiento llevaba a cabo los siguientes tratamientos de datos personales:

1.1 La grabación de las llamadas de la Guardia Urbana.
1.2 La grabación de las conversaciones mantenidas a través de los equipos de transmisiones asignado a cada agente.
1.3 La geolocalización de los terminales de comunicaciones de los agentes.
1.4 El enfoque de un puesto de trabajo mediante la cámara ubicada en la zona de atención al público de las dependencias policiales.

En relación a todos estos tratamientos, la entidad denunciante se cuestionaba si era necesario disponer de un registro de accesos, en el que constara la motivación de la consulta. A su vez, en lo que se refiere a la grabación de llamadas telefónicas y de las imágenes captadas por el sistema de videovigilancia instalado en las dependencias policiales, la entidad denunciante también se planteaba cuál era el plazo de conservación de los datos. Asimismo, la entidad denunciante consultaba si la persona que tiene acceso a las llamadas registradas "ha abierto uno expediente a algún trabajador, la llamada, se tiene la obligación de guardarla y adjuntarla el expediente" donde a una y si se pueden utilizar las imágenes captadas por el sistema de videovigilancia con fines disciplinarios. A su vez, la entidad denunciante indicaba que la cámara ubicada en la sala de atención al público (sala del operador) de la comisaría, enfocaría el puesto de trabajo del agente allí destinado. Y por último, la entidad denunciante manifestaba que el Ayuntamiento disponía de un documento de seguridad, al que quisiera acceder.

La entidad denunciante aportaba documentación diversa.

2. La Autoridad abrió una fase de información previa (núm. IP 351/2018), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes que concurrían.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

3. En fechas 21/02/2019 y 01/03/2019, la entidad denunciante complementó su escrito de denuncia. En síntesis, allí exponía lo siguiente:

3.1 Que en la Orden del Cuerpo 5/2017 se indicaba que una de las cámaras estaba en la entrada de las dependencias policiales, pero su ubicación estaba en la sala del operador, tal y como constaba en la correspondiente memoria.
3.2 Que se desconocía si se había dado de alta el archivo.
3.3 Que en la memoria del sistema de videovigilancia se indicaba que "No se colocan cámaras que enfocan puestos de trabajo."
3.4 Que el Inspector Jefe de la Guardia Urbana manifestó ante el Juzgado nº 1, "Previas 202/2018" que disponía de imágenes referidas al representante de la sección sindical denunciante.
3.5 Que el Inspector Jefe podía visionar las imágenes captadas por el sistema de videovigilancia instalado en las dependencias policiales a través de su móvil.
3.6 Que el administrador de la empresa instaladora de las cámaras sería el hermano del Inspector Jefe, por lo que consideraba que existía un presunto delito de prevaricación y de malversación de caudales públicos.

La entidad denunciante aportaba documentación diversa.

4. En esta fase de información, en fecha 16/04/2019, la Autoridad llevó a cabo un acto de inspección en las dependencias de la Guardia Urbana de (...), para verificar determinados aspectos relacionados con los tratamientos que realiza la Guardia Urbana. En ese acto de inspección presencial, los representantes del Ayuntamiento de (...) manifestaron, entre otros, lo siguiente:

4.1 Sobre las llamadas y la emisora:

ÿ Que se desconocía si funcionaba el programa que captaba las llamadas, entrantes y salientes, a través del número de la Policía Local.
ÿ Que las llamadas que se podrían registrar serían las efectuadas o mantenidas a través del número (...) (teléfono de la Guardia Urbana) y el teléfono de atención a la mujer ((...)).
ÿ Que respecto a las comunicaciones efectuadas a través de la emisora policial se desconocía si estaba activo la grabación de las llamadas.
ÿ Que el sistema de grabación de las llamadas a través de los números mencionados y de las comunicaciones efectuadas a través de la emisora de la Policía Local era el mismo.
ÿ Que la persona autorizada para acceder a dicho sistema era el Inspector Jefe de la Guardia Urbana.

4.2 Sobre la geolocalización de las emisoras de radio de la Guardia Urbana:

ÿ Que los terminales de comunicaciones policiales (emisora) permitían la geolocalización.
ÿ Que estos terminales son de la red RESCAT y permitían la geolocalización a través del SIPCAT.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

ÿ Que estos aparatos se disponían desde hace 6 años.
ÿ Que la geolocalización estaba en desuso, dado que fallaba a menudo.
ÿ Que la geolocalización estuvo en fase de pruebas durante unos días del verano de 2018. Al poco tiempo se desconectó.
ÿ Que la finalidad de geolocalización era garantizar la seguridad e integridad del personal y la adecuada prestación de los servicios policiales.
ÿ Que no se había utilizado con fines disciplinarios, ni de control laboral.
ÿ Que las personas usuarias que estaban autorizadas para acceder a la geolocalización eran el Inspector Jefe desde su inicio y un determinado sargento desde el verano del año 2018. El agente de sala tenía acceso a la geolocalización, dado que ésta sólo se podía consultar a través del monitor ubicado en la sala de control.
ÿ Que se desconocía si había un registro de accesos.

4.3 Sobre la cámara instalada en la sala de atención al público (operador):

ÿ Que la cámara se instaló en 2017.
ÿ Que se desconocía si la cámara permitía ampliar el campo de enfoque (zoom).
ÿ Que se desconocía el plazo de conservación de las imágenes.
ÿ Que la finalidad del tratamiento de imágenes a través de dicha cámara es garantizar la seguridad de las instalaciones y de los agentes. La instalación tuvo lugar a raíz de la alerta terrorista.
ÿ Que se desconocía si se habían utilizado o estaba previsto utilizar, las imágenes captadas con fines disciplinarios o de control laboral.
ÿ Que se desconocía si se conservaba alguna grabación de imágenes captadas a través del sistema de videovigilancia, referentes al representante de la entidad denunciante.
ÿ Que el usuario que estaba autorizado a acceder a las imágenes en tiempo real o grabadas era el Inspector Jefe.
ÿ Que se desconocía si las imágenes se podían visionar remotamente.

Asimismo, el personal inspector de la Autoridad verificó, entre otros, el siguiente:

ÿ Que en la sala de control o del operador había una cámara de videovigilancia. A su vez, también se constató que en el cristal de protección de la sala de control había un cartel informativo de la existencia de la cámara, que era visible desde el exterior de dicha sala.
ÿ Que el monitor, donde los representantes de la entidad inspeccionada manifestaban que se visionaba la geolocalización, estaba desconectado.
ÿ Que en el armario de comunicaciones (RAC) de las dependencias policiales, donde estaba el servidor, había varias salidas numeradas, entre ellas, la número 21. Según manifestaron los representantes del Ayuntamiento, estas salidas permitían la conexión entre el servidor y los distintos puntos físicos de conexión de los equipos informáticos (conexiones de red) distribuidos por las dependencias policiales que conforman su red interna. A su vez, el personal inspector constató que uno de los puntos físicos de conexión ubicado en la 2a planta de las dependencias policiales estaba numerado.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Por último, el personal inspector requirió a la entidad inspeccionada para que informara sobre diversos aspectos vinculados a los hechos denunciados.

5. En fecha 22/05/2019, el Ayuntamiento de (...) dio cumplimiento a este requerimiento mediante escrito a través del cual manifestaba lo siguiente:

5.1 Sobre las llamadas y la emisora:

ÿ Que en fecha 28/01/2013, se instaló en el RAC de comunicaciones de la Guardia Urbana un sistema de grabación de voz telefónico y radiofónico.
ÿ Que, en fecha 23/04/2019, se había comprobado que solo quedaban registradas las llamadas entrantes y salientes realizadas en el número de teléfono (...) (teléfono de la Guardia Urbana). Es decir, la grabación estaba limitada única y exclusivamente a llamadas efectuadas o recibidas desde la sala del operador.

ÿ Que la finalidad de este tratamiento es verificar y registrar convenientemente las demandas de los usuarios del servicio policial; así como de la respuesta y tratamiento que el agente-operador dispensa al requerimiento en cuestión, en casos en que exista un riesgo para la seguridad pública.
ÿ Que no se habían utilizado las conversaciones registradas con fines disciplinarios o de control laboral.

ÿ Que el plazo máximo de almacenamiento es de 30 días.
ÿ Que en relación al análisis de riesgos para determinar las medidas de seguridad adecuadas para mitigarlos, el Ayuntamiento estaba trabajando en la adecuación progresiva de la nueva legislación sobre protección de datos, que incluía un análisis de los riesgos.
ÿ Que se podía acceder al registro de llamadas, pero no quedaba constancia de quien había accedido dado que sólo había un funcionario autorizado para acceder. Desde el 23/04/2019 se habían dado de alta a tres funcionarios (mandos del cuerpo de la Guardia Urbana) como usuarios autorizados. A su vez, añadía que quedaba constancia de la identificación del usuario que accedía y del día y hora, pero no de la llamada que se consultaba.

ÿ Que no se verificaba con posterioridad si éstos eran necesarios para el ejercicio de sus funciones y para la finalidad declarada.
ÿ Que en relación a los números (...) y (...), no había conexión con la grabadora.

5.2 Sobre la geolocalización de las emisoras de radio de la Guardia Urbana:

ÿ Que el sistema a través del cual se podía consultar la geolocalización, no estaba auditado y carecía de registro de entradas y salidas de usuarios.
ÿ Que con anterioridad al período de pruebas (verano de 2018), la geolocalización no estaba activa. Sólo se habían realizado pruebas para verificar su correcto funcionamiento con resultado negativo. Se realizaron nuevas pruebas a partir del verano 2018, pero al persistir los errores, se desconectó definitivamente el sistema.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

5.3 Sobre la cámara instalada en la sala de atención al público (operador):

ÿ Que dada la capacidad interna del disco duro, el tiempo máximo de grabación es de unos 20 días aproximadamente, pasados los cuales las imágenes se borran de forma automática.
ÿ Que, en fecha 18/04/2019, se comprobó que no había ninguna grabación correspondiente al mes de marzo 2019, y los registros se iniciaban el día 01/04/2019 (se aportaban fotografías para acreditar dicha comprobación).
ÿ Que las grabaciones se conservan en la grabadora ubicada en el RAC del sistema informático. Se podían visionar por parte del Inspector Jefe de la Guardia Urbana.
ÿ Que no se habían utilizado, ni tampoco estaba previsto utilizar las imágenes captadas por dicha cámara con fines disciplinarios o de control laboral. La finalidad exclusiva es garantizar la seguridad y protección interior o exterior de estas dependencias, especialmente en un momento de alerta terrorista de nivel 4 sobre 5.
ÿ Que no se conserva ninguna grabación de imágenes captadas a través del sistema de videovigilancia, referentes al representante de la entidad denunciante.
ÿ Que las imágenes se pueden visionar desde el ordenador instalado en el despacho del Cap de Cos, y remotamente desde el teléfono móvil del Inspector en Cap.
ÿ Que para visionar las imágenes a través del móvil, es necesario introducir una contraseña para poder acceder a la aplicación (se aportaba una captura de pantalla). Las imágenes están encriptadas y con mancha de agua, a fin de garantizar que nadie autorizado pueda acceder a las mismas.
ÿ Que no constaba que existiera un registro de accesos, ya que había una sola persona autorizada a acceder a las imágenes.
ÿ Que no se verificaba con posterioridad si éstos eran necesarios para el ejercicio de sus funciones y para la finalidad declarada.

El Ayuntamiento de (...) aportaba copia de las imágenes grabadas el 15/04/2019, entre las 9:00 y las 9:02 horas.

6. En base a los antecedentes que se han relacionado y el resultado de las actuaciones de indagación llevadas a cabo en el marco de la información previa, a fecha de hoy se ha dictado un acuerdo de iniciación de procedimiento sancionador respecto a las conductas denunciadas relacionadas con el ámbito de visión de la cámara instalada en la sala del operador de la Guardia Urbana; y con la seguridad de los datos, por no haber efectuado un análisis de riesgos para determinar las medidas de seguridad apropiadas a aplicar en los tratamientos vinculados a la geolocalización; en el sistema de videovigilancia y en la grabación de las conversaciones telefónicas y de los equipos de transmisiones.

El resto de conductas denunciadas y otras consultas de la denunciante se abordan en esta resolución de archivo.

Fundamentos de derecho

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

1. De acuerdo con lo que prevén los artículos 90.1 de la LPAC y 2 del Decreto 278/1993, en relación con el artículo 5 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y el artículo 15 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, es competente para dictar esta resolución la directora de la 'Autoridad Catalana de Protección de Datos.

2. A partir del relato de hechos que se ha expuesto en el apartado de antecedentes, se deben analizar los hechos denunciados que son objeto de la presente resolución de archivo.

2.1. Acerca de las medidas de seguridad.

Al respecto, la entidad denunciante se cuestionaba si, para acceder a las conversaciones telefónicas o mantenidas a través de la emisora, a la geolocalización ya las imágenes grabadas por el sistema de videovigilancia instalado en las dependencias policiales, existía un registro de accesos donde se guardara a los que se ha accedido, la fecha y el motivo.

En el marco de las actuaciones previas la entidad denunciada ha indicado la información que se registra respecto a cada acceso, en los casos en los que se había implementado un registro de accesos (en la grabación de las conversaciones telefónicas y de la emisora ).

Dicho esto, hay que tener en cuenta que corresponde al responsable del tratamiento evaluar los riesgos inherentes al tratamiento y así determinar las medidas apropiadas para garantizar la seguridad de los datos, entre los que podría estar el registro de accesos (en el que se guardara la información que se considerase adecuada para garantizar la seguridad).

Así pues, sin haber efectuado esta evaluación no puede determinarse si esta medida (y su alcance) que indica la entidad denunciante es apropiada para garantizar la seguridad de los datos. Al respecto, hay que tener en cuenta que se ha acordado iniciar el correspondiente procedimiento sancionador, y una de las infracciones que allí se imputan es la de no haber efectuado dicho análisis de riesgos.

2.2. Sobre el plazo de conservación de los datos y bloqueo.

En el escrito de denuncia de 14/12/2018, en cuanto a la grabación de llamadas telefónicas y las imágenes grabadas por el sistema de videovigilancia, la entidad denunciante planteaba cuál sería el plazo de conservación de los datos y si éste era correcto.

El artículo 5.1.e del RGPD regula el principio de limitación del plazo de conservación, determinando que los datos personales serán "mantenidos de forma que permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

aplicación de las medidas técnicas organizativas apropiadas que impone el Reglamento ay

derechos y libertades de los interesados con el fin de proteger los

Así pues, el responsable del tratamiento debe conservar los datos durante el plazo estrictamente necesario para alcanzar la finalidad pretendida.

En el presente caso, el Ayuntamiento de (...) ha informado que el plazo máximo de almacenamiento de las llamadas entrantes y salientes efectuadas a través del número (...) es de 30 días como máximo, así como que el plazo de conservación efectivo de las imágenes captadas por el sistema de videovigilancia es de 18 días (aunque la previsión era que se conservaran las imágenes durante 20 días).

Considerando lo anterior, se considera que dichos plazos de conservación son adecuados para alcanzar las finalidades pretendidas. De hecho, en aplicación del principio de limitación del plazo de conservación de los datos, el artículo 22.3 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), establece que :

> "Los datos deben suprimirse en el plazo máximo de un mes desde la captación, excepto cuando se tengan que acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, en cuyo caso, se deben poner en conocimiento de la autoridad competente en un plazo máximo de 72 horas desde que tenga conocimiento de la existencia de la grabación."

Asentado lo anterior, procede abordar si existe alguna obligación de conservación de las llamadas telefónicas cuando éstas pueden constituir una prueba, tal y como plantea la entidad denunciante en su escrito de denuncia.

Al respecto, procede invocar el artículo 32 LOPDGDD. Los tres primeros apartados de este precepto disponen lo siguiente:

> "1. El responsable del tratamiento está obligado a bloquear los datos cuando lleve a término la rectificación o la supresión.
>
> El bloqueo de los datos consiste en la identificación y reserva de estos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluida la visualización, salvo para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.
>
> Transcurrido este plazo deben destruirse los datos.
>
> 3. Los datos bloqueados no se pueden tratar para ninguna finalidad diferente de la señalados en el apartado anterior."

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Así las cosas, el responsable del tratamiento está obligado a bloquear los datos cuando éstos deban rectificarse o suprimirse, con la finalidad exclusiva de ponerlos a disposición de los jueces y tribunales, el Ministerio Fiscal o las administraciones públicas competentes (entre ellas , las autoridades de protección de datos), para la exigencia de posibles responsabilidades que pudieran derivarse de las mismas durante el plazo de prescripción de las mismas.

Dicho esto, es preciso precisar que en el caso de tratamientos con fines de videovigilancia, la LOPDDDD ha establecido que no es aplicable la obligación de bloqueo (artículo 22.3).

2.3. Sobre la eventual incoación de un expediente disciplinario y documento de seguridad.

Seguidamente, en su escrito de 14/12/2018 la entidad denunciante plantea un caso hipotético, en el que se utilizaran las imágenes captadas por el sistema de videovigilancia instalado en las dependencias policiales con fines disciplinarios. Y, por otra parte, se exponía que el Ayuntamiento disponía de un documento de seguridad en relación con el sistema de videovigilancia, al que la entidad denunciante manifestaba que quería acceder.

Respecto a estas cuestiones, cabe evidenciar que no se denuncia ningún hecho concreto que comporte la eventual comisión de una concreta infracción de la normativa sobre protección de datos, sino que se sitúan en el ámbito de la consulta o de la mera hipótesis, motivo por lo que no procede entrar a analizarlos. Por este motivo, resulta innecesario abordarlos.

2.4. Acerca de la ubicación de las cámaras.

En su escrito de 01/03/2019, la entidad denunciante manifestaba que en la Orden del Cuerpo 5/2017 se indicaba que una de las cámaras estaba en la entrada de las dependencias policiales, pero su ubicación era en la sala del operador, tal y como constaba en la correspondiente memoria.

Pues bien, la Orden del Cuerpo 5/2017 de 16/05/2017 informaba que se había adquirido un sistema de videovigilancia y que la cámara controvertida estaría instalada en la "Entrada Jefatura, enfocando la zona de atención al público" .

Con posterioridad, en la memoria sobre el sistema de videovigilancia de las dependencias policiales, elaborada en fecha 22/05/2017 por el Ayuntamiento en cumplimiento de lo establecido en el artículo 10 de la Instrucción 1/2009, se concretaba que aquélla cámara estaría instalada "en el despacho del operador de la Guardia Urbana".

Así las cosas, con posterioridad a la Orden del Cuerpo 5/2017, el Ayuntamiento de (...) consideró instalar la cámara en otra ubicación (en la sala del operador).

De este cambio de ubicación de la cámara controvertida no se observa ninguna conducta contraria a la normativa sobre protección de datos.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Dicho esto, cabe indicar que la normativa sobre protección de datos no exige que se informe a las personas afectadas sobre la ubicación concreta de las cámaras.

Por otra parte, la entidad denunciante exponía que, en la mencionada memoria, el Inspector Jefe "manipula el informe, puestoque encuadra él lo que desea y lo que realmente la cámara está no enfocando" .

En relación a lo anterior, ciertamente en el artículo 10.1.e) de la Instrucción 1/2009 se señala que en la memoria debe hacerse referencia a la ubicación y campo de visión de las cámaras.

Pues bien, en la misma memoria que elaboró el Ayuntamiento en fecha 22/05/2017, en relación con el campo de enfoque de las cámaras, se especificaba lo siguiente: "Visionado orientativo: fotos realizadas con Iphone" .

Cabe decir que el hecho de que la memoria incluya este visionado orientativo no es contrario a la normativa sobre protección de datos. Y esto, porque esta memoria debe elaborarse con carácter previo a la puesta en marcha del sistema de videovigilancia (art. 10.1 de la Instrucción 1/2009).

Asentado lo anterior, debe tenerse en cuenta que se ha acordado iniciar el correspondiente procedimiento sancionador en relación al ámbito de visión de esta cámara.

2.5. Sobre la autorización y el archivo.

En este punto, también en el escrito de 01/03/2019, la entidad denunciante manifestaba desconocer si el sistema de videovigilancia había sido autorizado por la Comisión de Control de Dispositivos de Videovigilancia de Cataluña (en adelante CCDVC); así como si se había notificado el correspondiente archivo a la Autoridad.

En primer lugar, el artículo 7.2 del Decreto 134/1999, de 18 de mayo, de regulación de la videovigilancia por parte de la policía de la Generalidad y de las policías locales de Cataluña (en adelante, Decreto 134/1999) establece que la instalación de un sistema de videovigilancia fijo por parte de las policías locales, aparte de ser autorizada por la Dirección General de Administración de Seguridad del Departamento de Interior, requiere el informe previo favorable de la CCDVC.

No obstante, el artículo 1.3 del Decreto 134/1999 dispone que cuando la finalidad de las cámaras sea la de garantizar la seguridad y protección interior o exterior en inmuebles, dependencias o instalaciones de las policías locales, tal y como sucede en el presente caso, en relación a los tratamientos efectuados en dichos recintos policiales, no será de aplicación dicha normativa sectorial.

Así pues, en el presente caso no será exigible el informe favorable de la CCDVC.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Y en segundo lugar, en lo referente a la notificación e inscripción del fichero a la Autoridad, es necesario poner de manifiesto que el RGPD ha eliminado esta obligación.

2.6. Acerca del acceso a las imágenes.

Al respecto, la entidad denunciante exponía que, en instancias judiciales, el Inspector Jefe habría declarado que disponía imágenes de la persona representante de la entidad denunciante captadas por la cámara ubicada en la sala del operador. Dado lo anterior solicitaba a la Autoridad que pidiera al Ayuntamiento una copia de dichas imágenes.

En primer lugar, hay que poner de manifiesto que esta petición debe formalizarse mediante una solicitud de acceso que, la persona interesada, debe dirigir al responsable del tratamiento (el Ayuntamiento) de conformidad con lo previsto en el artículo 15 RGPD. Y en caso de que el Ayuntamiento no atienda esta solicitud o la respuesta no sea satisfactoria, la persona interesada puede presentar una reclamación ante la Autoridad.

Sin perjuicio de lo anterior, por medio de escrito de 21/05/2019, el Ayuntamiento de (...) manifestó que no se conservaban las imágenes referidas.

2.7. Sobre el visionado de imágenes mediante el móvil.

En este punto, la entidad denunciante manifestaba que el Inspector Jefe podría visionar las imágenes captadas por el sistema de videovigilancia.

En este sentido, por medio de escrito de 21/05/2019, el Ayuntamiento de (...) informó que el Inspector Jefe era la única persona autorizada por el Consistorio para acceder a las imágenes captadas y grabadas por el sistema de videovigilancia instalado en las dependencias policiales; así como que éste podía visionarlas a través de su ordenador ubicado en las dependencias policiales y, remotamente, a través de su móvil.

A su vez, señalaba que para visualizar las imágenes a través del móvil es necesario "introducir una contraseña con el fin de garantizar que [illegible] no a la aplicación, y las imágenes [illegible] a las mismas."

Así las cosas, el acceso por parte de una persona autorizada a las imágenes captadas y grabadas por el sistema de videovigilancia, o remotamente, en el ejercicio de sus funciones, no es contrario a la normativa de protección de datos.

Otra cosa es si este tratamiento garantiza la seguridad de los datos. En este sentido, es necesario llevar a cabo el análisis de riesgos, cuya carencia se imputa al Ayuntamiento en el procedimiento sancionador que se ha incoado.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

2.8. Sobre los hechos delictivos.

Por último, en su escrito de 01/03/2019, la entidad denunciante manifestaba que el administrador de la empresa instaladora de las cámaras sería el hermano del Inspector Jefe, por lo que consideraba que se podría haber cometido un presunto delito de prevaricación y malversación de caudales públicos.

En relación con lo anterior, es suficiente indicar que esta Autoridad no es competente para dirimir si estos hechos son o no constitutivos de delito.

3. De conformidad con todo lo expuesto en el fundamento de derecho 2º, y dado que durante las actuaciones llevadas a cabo en el marco de la información previa no se ha acreditado, en relación con los hechos que se han abordado en esta resolución, ningún hecho que pueda ser constitutivo de alguna de las infracciones previstas en la legislación aplicable, procede acordar su archivo.

Resolución

Por tanto, resuelvo:

1. Archivar las actuaciones de información previa número IP 351/2019, relativas al Ayuntamiento de (...), en lo referente a los hechos dirimidos al fundamento de derecho 2º.

2. Notificar esta resolución al Ayuntamiento de (...) y comunicarla a la entidad denunciante.

3. Ordenar la publicación de la resolución en la web de la Autoridad (www.apd.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con el artículo 14.3 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, entidad denunciada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos, en el plazo de un mes a contar desde el día siguiente al de su notificación, de acuerdo con el que prevé el artículo 123 y siguientes de la Ley 39/2015. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Asimismo, la entidad denunciada puede interponer cualquier otro recurso que considere conveniente para defender sus intereses.

La directora,