- **Procedimiento Nº: PS/00027/2019**

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 22/05/2018 tuvo entrada una reclamación de ***A.A.A.*** contra la COMISARIA PROVINCIAL DE ******LOCALIDAD.1*** DEL CUERPO NACIONAL DE POLICÍA por uso de imágenes del sistema de videovigilancia de la Comisaria para incoarle un procedimiento disciplinario, con desvío de la finalidad propia del sistema y sin que hubiese sido informado de que dicho dispositivo pudiera ser empleado para dicha finalidad, además de la falta de proporcionalidad en cuanto al uso del mismo.

El reclamante, Inspector del CNP, es ******PUESTO.1*** de un grupo de policías de la ******BRIGADA.1*** de la Comisaria de ******LOCALIDAD.1***, manifiesta que realiza sus funciones a turnos rotatorios y de uniforme adscrito a la Brigada de Seguridad Ciudadana. La noche del ******FECHA.1*** prestaba servicio y a las 23:30 acudieron el Inspector ******PUESTO.2*** de la Brigada Provincial de Seguridad Ciudadana, ***B.B.B.*** con el ******PUESTO.1*** (jefe de la Comisaria). En ese momento, los policías se prestaban a cenar, vistiendo el reclamante un forro polar negro sobre el uniforme, debido al frío en las dependencias. Captadas imágenes por el sistema de vigilancia de detenidos de la Comisaria en las que figura como se menciona, las imágenes se han utilizado para instruirle un procedimiento disciplinario. Matiza el reclamante que esa noche no había ningún detenido, y que las imágenes fueron solicitadas por el Inspector ******PUESTO.2*** el ******FECHA.3*** para "*poder sancionar al reclamante por llevar incorrecta la uniformidad*", al funcionario encargado de las telecomunicaciones que procedió el ******FECHA.2*** y que el uso de las mismas para este fin no es adecuado, pues además existían otros funcionarios presentes que podían haber testificado sobre el hecho.

Existe la instrucción del Ministerio de Interior 12/2015 que señala que en los centros de detención debe existir un sistema de videovigilancia para garantizar la seguridad física de las personas privadas de libertad y de los funcionarios que ejercen su custodia.

Aporta copia parcial (tachados algunos extremos para imposibilitar su lectura completa) de:

1) Acta declaración prestada por el Inspector ******PUESTO.2, B.B.B.,*** de ******FECHA.3***, como "*denunciado*", "*diligencias* ******DILIGENCIA.1*** *en relación con denuncia de "acoso laboral*" instado por el reclamante. En dicha declaración, de la que se deriva que se relaciona con actuaciones judiciales, el Inspector manifiesta que vio al reclamante la noche del ******FECHA.1*** porque fue a entregarle la denegación de un permiso y le vio sin la

uniformidad reglamentaria, y le amonestó, y de cara a poder probarlo, ya que era reincidente, a la mañana siguiente solicitó al responsable de telecomunicaciones copia de las imágenes obtenidas por las cámaras próximas al vestíbulo de su despacho, para comprobar si había modificado su conducta y cumplido la orden. "*Como quiera que posteriormente causó baja laboral, es por lo que no se ha tramitado ninguna actuación disciplinaria*".

2) Acta de declaración (también hay tachado en el escrito numerosos párrafos en el mismo asunto) del Comisario, en calidad de testigo, que manifiesta que el Inspector ***PUESTO.2*** le comentó la falta de uniformidad del reclamante y a la mañana siguiente el Inspector le informó que había solicitado la grabación de las cámaras del hall de la Comisaria al objeto de comprobar si finalmente había cumplido la orden.

3) Acta de declaración del encargado de telecomunicaciones, como testigo, que indica que recibió la orden de obtener copia de las imágenes de la franja horaria entre las 0 horas y las 4 horas del ******FECHA.2***, "*conociendo posteriormente que el objeto de dicha petición era comprobar si el* ******PUESTO.1*** *vestía el uniforme reglamentario*".

Aporta copia de acta de entrega de grabaciones de ******FECHA.2*** a instancia del Inspector ***PUESTO.2***

SEGUNDO**:** A la vista de los hechos denunciados, por la Subdirección General de Inspección de Datos, se traslada la denuncia a la DIRECCIÓN GENERAL DE LA POLICÍA, para que *remitan a esta Agencia la documentación relevante relativa a los trámites llevados a cabo por el responsable de tratamiento, en relación con los hechos expuestos en la reclamación, incluyendo en particular la siguiente información:*

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, de acuerdo con lo previsto en el artículo 12 del RGPD, se han tomado las medidas oportunas para facilitar al afectado el ejercicio de sus derechos en virtud de los artículos 15 a 22, incluyendo copia íntegra de las comunicaciones remitidas en respuesta a las solicitudes efectuadas.

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

La Dirección General de la Policía, con fecha 3/08/2018 y sobre la utilización de cámaras de videovigilancia de la Comisaría Provincial de ******LOCALIDAD.1***, manifiesta

a) Se adjunta informe de la Unidad de Informatica y Comunicaciones de la Jefatura Central de Logística e Innovación de la Dirección General de la Policía. En ella se informa que "*La gestión de los equipos de CCTV instalados en los calabozos de la Comisaria de* ******LOCALIDAD.1*** *se realiza desde la propia comisaria*" y continúa dando detalles de dicho sistema.

TERCERO: Con fecha 5/09/2018, el reclamado indica que no ha recibido respuesta por parte del delegado de protección de Datos, y el 5/12/2018 otro escrito en el que indica que no ha recibido respuesta de la AEPD.

El mismo tipo de escrito del reclamante sobre que no ha recibido respuesta tiene entrada los días 21/02/2019 y 13/03/2019.

Con fecha 4/03/2019 se le envió escrito informando de la situación de su denuncia.

CUARTO: Con fecha 1/04/2019 se acordó por la directora de la AEPD:

"*iniciar procedimiento sancionador al Ministerio del Interior-Dirección General de la Policía (Comisaria Provincial de* ******LOCALIDAD.1*** *del Cuerpo Nacional de Policía) por la presunta infracción del artículo 5.1.b) del RGPD, infracción tipificada en el artículo 83.5 a) del RGPD.*

En el envío cursado a través de la plataforma de nofitic@, se certifica:

"*El servicio de Soporte del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada CERTIFICA:*

- Que el Ministerio de Política Territorial y Función Pública (a través de la Secretaría General de Administración Digital) es, actualmente, el titular del Servicio de Notificaciones Electrónicas (SNE) y Dirección Electrónica Habilitada (DEH) de acuerdo con la Orden PRE/878/2010 y el Real Decreto 769/2017, de 28 de julio. El prestador de dicho servicio desde el 26 de junio de 2015 es la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), según Encomienda de Gestión en vigor del Ministerio de Hacienda y Administraciones Públicas.
-Que a través de dicho servicio se envió la notificación:
Referencia: 94162555ca5cd5c8ab84 Administración actuante: Agencia Española de Protección de Datos (AEPD) Titular: DIRECCION GENERAL DE LA POLICIA-SERVICIOS CENTRALES-MIR - S2816015H

Asunto: "Notificación disponible en la Carpeta o DEH del titular indicado" con el siguiente resultado:

Fecha de puesta a disposición: 07/04/2019 05:00:38
Fecha de rechazo automático: 15/04/2019 00:00:00
El rechazo automático se produce, de forma general, tras haber transcurrido diez días naturales desde su puesta a disposición para su acceso según el párrafo 2, artículo 43, de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Y de forma particular, superado el plazo establecido por la Administración actuante de acuerdo a la normativa jurídica específica que sea de aplicación.

La LPCAP añade en su artículo 14" *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas* "

2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas."

Y se concreta en el artículo 41" *Condiciones generales para la práctica de las notificaciones "1. Las notificaciones se practicarán preferentemente por medios electrónicos y, en todo caso, cuando el interesado resulte obligado a recibirlas por esta vía.*

No obstante, lo anterior, las Administraciones podrán practicar las notificaciones por medios no electrónicos en los siguientes supuestos:

a) Cuando la notificación se realice con ocasión de la comparecencia espontánea del interesado o su representante en las oficinas de asistencia en materia de registro y solicite la comunicación o notificación personal en ese momento.

b) Cuando para asegurar la eficacia de la actuación administrativa resulte necesario practicar la notificación por entrega directa de un empleado público de la Administración notificante.

Con independencia del medio utilizado, las notificaciones serán válidas siempre que permitan tener constancia de su envío o puesta a disposición, de la recepción o acceso por el interesado o su representante, de sus fechas y horas, del contenido íntegro, y de la identidad fidedigna del remitente y destinatario de la misma. La acreditación de la notificación efectuada se incorporará al expediente."

Como consecuencia, la notificación del acuerdo se entiende producida con todos los efectos jurídicos.

QUINTO: Se obtiene copia de la web de la instrucción 1/2012 de 1/10/2015, (numerada como 12/2015) de la Secretaría de Estado de Seguridad, (SES) por la que se aprueba el "*protocolo de actuación en las áreas de custodia de detenidos de las fuerzas y cuerpos de seguridad del estado*". Queda incorporada al expediente como objeto asociado 2 en la aplicación que gestiona el mismo.

En la misma figura: 2 f. Videovigilancia: Los centros de detención de las Fuerzas y Cuerpos de Seguridad del Estado dispondrán de sistemas de videovigilancia con grabación que contribuyan a garantizar la integridad física y la seguridad de las personas privadas de libertad y la de los funcionarios policiales que ejercen su custodia. Dicha grabación deberá estar permanentemente activa, con independencia de que los agentes encargados de la custodia deban mantener un control permanente de los calabozos a través de los medios de videovigilancia.

Los sistemas de videovigilancia se regirán por lo que establece la Ley Orgánica 4/1997, de 4/08, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. En ningún caso, podrán permitir la visualización de las zonas de aseo, con el fin de preservar la intimidad de las personas detenidas.

Se obtiene copia en internet de la instrucción núm. 4/2018, firmada el 14/05/2018 de la SES por la que se aprueba la actualización del "p*rotocolo de actuación en las áreas de*

custodia de detenidos de las Fuerzas y Cuerpos de Seguridad del Estado" y se deja sin efecto la instrucción 12/2015. Queda incorporada al expediente como objeto asociado 1 en la aplicación que gestiona el mismo.

Figura en su punto 2.f):

"*Videovigilancia: Los centros de detención de las Fuerzas y Cuerpos de Seguridad del Estado dispondrán de sistemas de videovigilancia y grabación, que permitan el visionado en las condiciones de luz de sus habitáculos, para garantizar la integridad física y la seguridad de las personas privadas de libertad y la de los funcionarios policiales que ejercen su custodia.*

Dicha grabación deberá estar permanentemente activa, con independencia de que los agentes encargados de la custodia deban mantener un control de los calabozos a través de los medios de videovigilancia.

*Las grabaciones serán conservadas durante treinta días a partir de su captación. Una vez finalizado dicho plazo serán destruidas, salvo que se produzca algún incidente en el transcurso de la custodia de un detenido o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública; con una investigación policial en curso o con un procedimiento judicial o administrativo abierto. En estos casos, la grabación se conservará a disposición de las Autoridades competente*s."

SEXTO: Dentro del periodo de pruebas se notifica a la reclamada el 24/06/2019 el inicio del periodo de pruebas, solicitando:

-Croquis de Comisaria de ******LOCALIDAD.1*** en la que sucedieron los hechos, en el que se vea la situación en la que está colocada la cámara que sirvió para recoger la imagen del reclamante y tipo de habitación en la que se recogieron y se seleccionaron las imágenes. Imagen en color del campo que recoge dicha cámara identificando los espacios hacia los que enfoca.

-Indicar si se ha entregado a los funcionarios que prestan servicios de custodia y guarda de detenidos en alguna ocasión una guía explicando el uso o finalidad de estas cámaras, y si se les ha informado que pueden ser objeto de sanción disciplinaria, en que supuestos, modo en que se les ha informado. En concreto al reclamante.

-Si conoce si el reclamante ha sido sancionado, copia de la resolución, copia de documentos que obren en el procedimiento, y si le consta su impugnación administrativa y (/o judicial).

-Posición/jerarquía que ostentaba la persona que solicita la extracción de las imágenes, y si la Dirección General de la Policía ha emitido alguna instrucción sobre la petición de datos de los sistemas de videovigilancia, procedimientos a seguir en la petición de dichos datos, registro de las peticiones, a quien corresponde decidir si se entregan o no, o si estima conveniente su preparación.

- Si a nivel disciplinario, la persona que solicitó la extracción de imágenes puede iniciar un procedimiento disciplinario, tramites que debe llevar a cabo.

Se le remite copia del acuerdo de inicio con objeto de que de su lectura y conocimiento y con lo que se le solicita aporte lo solicitado y alegue lo que en su caso considere oportuno.

Recibido el envío, con fecha 8/07/2019, la reclamada presenta escrito en el que sin responder a lo que se cuestiona, aporta:

a) informe elaborado por la Comisaria provincial de ******LOCALIDAD.1***, asunto; "*remitiendo informe sobre uso CCTV para fines disciplinarios*" firmado por el Inspector ***PUESTO.2*** Sr. ***B.B.B.***, el 2/01/2019. En el mismo destaca:

> -"*A las 23,30 horas del pasado* ******FECHA.1*** *se presentó en el despacho del* ******PUESTO.1*** *de la comisaria…(reclamante) comprobando según el mismo inspector reconoce en su declaración que este se encontraba de paisano, dos horas después de haber comenzado el servicio" le recriminó el hecho y le ordenó que se pusiera el uniforme", "él tenía conocimiento de que el citado no vestía el uniforme durante los turnos de noche pero carecía de pruebas" "En previsión de que volviera a incumplir la orden de prestar su servicio uniformado, solicitó formalmente al responsable del sistema de CCTV que visionara las imágenes de la noche del* ******FECHA.1*** *desde las 23,45 para comprobar si se había cambiado y en caso contrario, extrajera las imágenes precisas para dar cuenta al Comisario de dicho hecho y poder probarlo". "El Inspector -reclamante- se dio de baja médica desde* ******FECHA.4*** *y a continuación le denunció a por acoso laboral y por infracciones de la LO 4/2010 del reglamento de régimen disciplinario por infringir la legislación sobre uso de videocámaras. "Ambas denuncias fueron archivadas" por la unidad de despacho administrativa. En el escrito indica que se trata de cámaras cuyas imágenes se obtienen y usan por las fuerzas y cuerpos de seguridad del estado, y que se rigen por las disposiciones sobre la materia. Señala los informes de 2009 números 286, 472 de la AEPD sobre la posibilidad de usar grabaciones del sistema de CCTV instalado en dependencias policiales como medios de prueba para exigir responsabilidades disciplinarias, se indica que "carece de competencias para valorar que pruebas pueden o no aportarse a un procedimiento disciplinario" Indica que la finalidad del sistema es la seguridad de la comisaria y protección interior y exterior del edificio, por lo que considero que si bien "están instaladas para tal fin, este no excluye su uso para poder verificar y comprobar hechos objeto de una investigación, por lo que era pertinente, legal, justificado y proporcionado usarlo para probar y así poder depurar responsabilidades disciplinarias si las hubiera", se limitaba a unas cámaras cuya finalidad es la seguridad pública y el control de entradas y salidas de ciudadanos incluyéndose por tanto los horarios de prestación del servicio* "

Se asocia al procedimiento el informe número 286/2009 del Gabinete Jurídico de la AEPD, firmado por Abogado del Estado de 12/06/2009, hallado en la aplicación SIJ que gestiona dichos informes, que figura con el siguiente literal:

> *Ref. de entrada 177676/2009(Sección Sindical S.E.P.-CV del Ayuntamiento de* Benidorm)

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por la Sección Sindical S.E.P.-CV del Ayuntamiento de Benidorm, cúmpleme informarle lo siguiente:

La consulta plantea varias cuestiones relacionadas con la instalación de sistemas de videovigilancia por el Ayuntamiento de Benidorm, para comprobar si se ajustan a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

La primera cuestión plantea si el Ayuntamiento ha recabado autorización de la Agencia Española de Protección de Datos para instalar el sistema de videovigilancia en el edificio de la policía local. Sobre este punto, se comunica que la Agencia Española de Protección de Datos carece de competencias para la autorización de sistemas de videovigilancia, siendo su competencia la de velar por que el tratamiento de datos derivado de la existencia de dichos sistemas resulte acorde a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y la Instrucción 1/2006, de 8 de noviembre de esta Agencia.

No obstante, podemos señalar que el referido Ayuntamiento notificó y tiene inscrito en el Registro General de Protección de Datos, un fichero de cámaras de videovigilancia de la Policía, cuyo nombre y finalidad declarada es "El control de acceso y vigilancia del edificio de la Policía" y "videovigilancia".

En la declaración del mencionado fichero, consta que la Disposición General de creación del fichero se publicó en el Boletín de la Provincia, con el número 00067 y fecha de 9 de abril de 2008.

En cuanto al período de conservación de las imágenes, atendiendo a la finalidad descrita en la Disposición de creación del fichero, resulta de aplicación la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras donde se prevé en su artículo 6 que "Los datos serán cancelados en el plazo máximo de un mes desde su captación."

Respecto al plazo que pueden conservarse las imágenes la Agencia se ha pronunciado en el informe de 3 de julio de 2008, en cuanto al fundamento de dicho plazo señalando que

> *"El artículo 6 de la instrucción 1/2006, donde se regula el plazo de conservación de las imágenes está íntimamente relacionado con lo dispuesto en el artículo 4.5 de la Ley Orgánica 15/1999 que señala lo siguiente "Los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.", dicha previsión se reitera en el artículo 8.6 del Reglamento de desarrollo de la Ley Orgánica. El criterio de la Agencia atendiendo a dicho principio ha sido entender que las imágenes grabadas para cumplir con la finalidad de seguridad deben de conservarse como máximo durante un mes, una vez cumplida dicha finalidad, éstas deben de cancelarse. Por lo que dicho plazo sigue vigente tras la entrada en vigor del Reglamento dado que no se opone a las previsiones contenidas en el mismo.*

A mayor abundamiento es preciso destacar que el plazo de un mes que en la Instrucción se establece para cancelar las imágenes, no es arbitrario, dado que se ha optado por seguir el mismo criterio que el fijado en la Ley Orgánica 4/1997, de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos, que en su artículo 8 señala que "Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación".

Por otro lado la instrucción señala expresamente en el artículo 6 que "los datos serán cancelados en el plazo máximo de un mes desde su captación", quiere esto decir que una vez transcurrido dicho plazo las imágenes deberán de ser canceladas, lo que implica el bloqueo de las mismas pues así lo establece, la Ley Orgánica 15/1999 que en el artículo 16.3 señala que "la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".

La consulta, plantea también si la omisión del deber de informar de los derechos de acceso, rectificación, cancelación y oposición de los datos convierte en ilegales las cámaras. Para que la instalación de dichas cámaras se ajuste a lo dispuesto en la normativa de protección de datos, se exige el cumplimiento de determinados requisitos tales como; la legalidad del tratamiento de las imágenes. El artículo 6.1 de la Ley Orgánica 15/1999 al que se remite el artículo 2 de la Instrucción 1/2006, establece que "El tratamiento de datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa". Lo que obliga acudir a una Ley que prevea el tratamiento de las imágenes sin recabar el consentimiento del afectado.

En este sentido, La ley Orgánica 2/1986, de 13 marzo de Fuerzas y Cuerpos de Seguridad en su artículo 11, regula sus funciones señalando que "1. Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: (..) c) Vigilar y proteger los edificios e instalaciones públicos que lo requieran", en consecuencia, podemos concluir que la Ley Orgánica 2/1986, legitima el tratamiento de las imágenes recabas en las dependencias policiales.

Asimismo deberá cumplirse con el deber de informar conforme a lo dispuesto en el artículo 3 de la Instrucción 1/2006, y notificar e inscribir el fichero en el Registro General de Protección de Datos. Además de permitir el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, en los términos del artículo 5 de la Instrucción. En el ejercicio de los derechos deberá de tenerse en cuenta las especialidades del artículo 23 de la Ley Orgánica 15/1999, pues se regulan las excepciones a los derechos de acceso, rectificación y cancelación en los ficheros de los que sea responsable las Fuerzas y Cuerpos de Seguridad del Estado.

Por último se plantea, si las grabaciones obtenidas a través del sistema de videovigilancia instalado en las dependencias de la policía local, pueden ser utilizadas como medios de prueba para exigir a los policías responsabilidades disciplinarias. Sobre este punto, hay que indicar que la Agencia, carece de competencias para valorar qué pruebas o no pueden aportarse en un procedimiento disciplinario.

No obstante, según la finalidad declarada en el Registro General de Protección de Datos, el fichero creado es para controlar y vigilar el acceso al edificio, por ello, si las responsabilidades disciplinarias, fueran derivadas del acceso al mismo (horario de entrada y salida por parte de los policía) sí podrían ser utilizadas, no pudiendo ser utilizadas para otro tipo de finalidades, que no consten declaradas.

Por último, para el caso de que por el consultante se plantee la existencia de una actuación presuntamente contraria a la Ley Orgánica 15/1999, deberá dirigir su denuncia ante este mismo organismo, con la finalidad de que se adopten las medidas necesarias a fin de comprobar si procede o no la apertura del correspondiente expediente sancionador siendo así que el artículo 37.1.g) de la Ley atribuye a esta Agencia la potestad sancionadora en materia de protección de datos.

En todo caso las alegaciones efectuadas por el denunciante deberían contener la documentación acreditativa de la efectiva realidad de los hechos. Dicha denuncia deberá presentarse por escrito y dirigirse a la Agencia Española de Protección de Datos en los términos que establece el artículo 70 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, debiendo contener:

a) Nombre y apellidos del interesado y, en su caso, de la persona que lo represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones.
b) Hechos, razones y petición en que se concrete, con toda claridad, la solicitud.
c) Lugar y fecha.
d) Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio.
e) Órgano, centro o unidad administrativa a la que se dirige. (en su caso sería la subdirección General de Inspección de Datos de esta Agencia"

Se asocia al procedimiento el Informe 472/2009 de Abogado del Estado, de 20/10/2009:

Ref. de entrada ******REFERENCIA.1 (Fundación ***FUNDACIÓN.1)***

"*Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por la* ******FUNDACIÓN.1****, cúmpleme informarle lo siguiente:*

La consulta plantea varias cuestiones relacionadas con los temas de videovigilancia, para adecuar su actuación tanto a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, como al Reglamento de desarrollo de la misma y a la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

La primera pregunta, alude a la obligación de conservar las imágenes bloqueadas, a este respecto, debe señalarse que el período de conservación de las imágenes, según el artículo 6 de la Instrucción 1/2008 que "Los datos serán cancelados en el plazo máximo de un mes desde su captación."

Respecto al plazo que pueden conservarse las imágenes la Agencia se ha pronunciado en el informe de 3 de julio de 2008, en cuanto al fundamento de dicho plazo señalando que

> *"El artículo 6 de la instrucción 1/2006, donde se regula el plazo de conservación de las imágenes está íntimamente relacionado con lo dispuesto en el artículo 4.5 de la Ley Orgánica 15/1999 que señala lo siguiente "Los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.", dicha previsión se reitera en el artículo 8.6 del Reglamento de desarrollo de la Ley Orgánica. El criterio de la Agencia atendiendo a dicho principio ha sido entender que las imágenes grabadas para cumplir con la finalidad de seguridad deben de conservarse como máximo durante un mes, una vez cumplida dicha finalidad, éstas deben de cancelarse. Por lo que dicho plazo sigue vigente tras la entrada en vigor del Reglamento dado que no se opone a las previsiones contenidas en el mismo.*
>
> *A mayor abundamiento es preciso destacar que el plazo de un mes que en la Instrucción se establece para cancelar las imágenes, no es arbitrario, dado que se ha optado por seguir el mismo criterio que el fijado en la Ley Orgánica 4/1997, de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos, que en su artículo 8 señala que "Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación".*
>
> *Por otro lado la instrucción señala expresamente en el artículo 6 que "los datos serán cancelados en el plazo máximo de un mes desde su captación", quiere esto decir que una vez transcurrido dicho plazo las imágenes deberán de ser canceladas, lo que implica el bloqueo de las mismas pues así lo establece, la Ley Orgánica 15/1999 que en el artículo 16.3 señala que "la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".*

Por otro lado, el Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, define en su artículo 5.1. b) la cancelación como "Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos."

En cuanto al modo de llevar a cabo el bloqueo, se señalaba en informe de esta Agencia de 5 de junio de 2007 que "deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de

los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia."

En cuanto al plazo de conservación de las imágenes bloqueadas, no podemos sino volver a reiterar lo manifestado en el informe que adjunta la entidad consultante de 18 de febrero de 2009 en el que se señala "resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave."

Y en cuanto a la última cuestión planteada, es preciso distinguir si el régimen de grabaciones se efectúa en soporte digital o no, pues en el caso de que se efectúe en soporte digital, existe un tratamiento automatizado de datos, que implica la obligatoriedad de cumplir con las medidas de seguridad de nivel básico previstas en el artículo 94 del Reglamento de desarrollo de la Ley Orgánica 15/1999."

b) Copia de Informe de la Subdirección General de Logística e Innovación de 3/12/2018, destinatario "*delegado de protección de datos. Gabinete Técnico*"

En el mismo se habla ahora del fichero de "*videovigilancia*" para la finalidad de "*garantizar la protección interior y exterior de las Comisarias del CNP y de los edificios, instalaciones y centros vigilados por el mismo, Su uso está dirigido a la "seguridad y protección*". El sistema se regula por la Orden interna 1865 de 30/11/2016 del Ministerio de Interior por la que se modifica la Orden INT/1202/2011, de 4/05, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, BOE 12/12/2016. En el artículo único se indica que tanto la nueva creación de los ficheros que se contienen como la modificación, se rige por la LOPD y normativa de desarrollo.

En el mismo se crea el fichero: "*Videovigilancia"* del que destacan:

a.2) *Finalidad: Garantizar la seguridad y protección interior y exterior de las Comisarías del Cuerpo Nacional de Policía y de los edificios, instalaciones y centros vigilados por el mismo*.

a.3) Usos previstos: Seguridad y protección.

b) Origen de los datos:

b.1) Colectivo: Personas que se encuentren en zonas videovigiladas de las Comisarías del Cuerpo Nacional de Policía o de los edificios, instalaciones y centros vigilados por el mismo.

b.2) Procedencia y procedimiento de recogida: Circuito cerrado de televisión.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: Imagen/voz.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: órganos judiciales, Ministerio Fiscal y otros servicios del Cuerpo Nacional de Policía para el ejercicio de las funciones legalmente encomendadas, así como a otras Fuerzas y Cuerpos de Seguridad para el ejercicio de sus funciones de protección de la seguridad pública, conforme a lo establecido en el artículo 22.2 de Ley Orgánica 15/1999, de 13 de diciembre, en cumplimiento de los principios de colaboración, mutuo auxilio y cooperación e información recíprocas que establece la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Subdirección General de Logística, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Subdirección General de Logística, calle Julián González Segador, sin número, 28043 Madrid.

i) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Añade que "*En la actualidad el área de telecomunicaciones de la unidad de informatica y comunicaciones dispone de un procedimiento para el tratamiento de imágenes de videovigilancia donde se determinan los siguientes aspectos:" El sistema de control de accesos a las imágenes, constan de una clave alfanumérica con dos categorías de usuarios: administrador con permisos para visionado y extracción de imágenes y usuario básico solo con permisos para visionado. Los delegados TIC poseen los permisos de administración de usuarios y por tanto para la extracción de imágenes en todas las comisarias provinciales del CNP*"

SÉPTIMO: Con fecha 18/09/2019 se da respuesta a escrito del reclamante que solicita se le informe de la situación del procedimiento, pide ser considerado interesado en el mismo, decidiendo comunicarle el final del procedimiento a efectos de la consulta en web de la resolución.

OCTAVO: Con fecha 18/11/2019 se emitió propuesta de resolución con el literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione con apercibimiento a la* DIRECCION GENERAL DE LA POLICIA (MINISTERIO DEL INTERIOR), *por una infracción del Artículo 5. 1 b) del RGPD, tipificada en el Artículo 83.5 del RGPD*."

La reclamada presenta alegaciones indicando que los hechos sucedieron antes de la entrada en vigor del RGPD, y ello es importante pues "*Durante el periodo de vigencia de la anterior LOPD los Tribunales han mantenido que el uso de imágenes procedentes de las Cámaras de comisarias para comprobar el correcto funcionamiento de los servicios policiales no puede considerarse una finalidad incompatible prohibida por la Ley, aunque su uso principal sea la seguridad de los bienes y de las personas*".

HECHOS PROBADOS

1) El Inspector ******PUESTO.2*** de la Brigada provincial de seguridad Ciudadana de la comisaria de ******LOCALIDAD.1***, Sr ***B.B.B.***, observa la noche del ******FECHA.1*** que el reclamante, Inspector del CNP y ******PUESTO.1***, no va debidamente uniformado, llevando un forro polar negro según declara el reclamante, siendo amonestado por él y conminado a uniformarse debidamente, según declara el Inspector ******PUESTO.2***, abandonando el lugar. Al día siguiente, el Inspector ******PUESTO.2***, decide verificar si el reclamante cumplió su orden y solicita copia de las imágenes de las cámaras entre las 0 y las 4 del día ******FECHA.2***. La extracción de las imágenes se produce por personal dedicado a telecomunicaciones en la misma comisaria de ******LOCALIDAD.1***, personal que manifestó, que no se contenía ni se explicitaba motivo alguno, conociéndose después *que el objeto de dicha petición era comprobar si el* ******PUESTO.1*** *vestía el uniforme reglamentario*". No se dispone de la petición escrita, si la hubiera de extracción de las imágenes, y se aporta copia de acta de entrega de grabaciones de ******FECHA.2***, a instancia del Inspector ******PUESTO.2***

2) Según manifiesta el reclamante la noche del ******FECHA.1*** no había ningún detenido en la Comisaria.

3) La Comisaria del CNP de ******LOCALIDAD.1*** en la que presta servicios el reclamante, dispone de cámaras de videovigilancia para las celdas de los detenidos. Se rige dicha captación por el protocolo de actuación en las Áreas de Custodia de Detenidos de las Fuerzas y Cuerpos de Seguridad del Estado, instrucción de la Secretaria de Estado de Seguridad 4/2018, firmada el 14/05/2018 y que deja sin efecto la Instrucción número 12/2015 de la Secretaría de Estado de Seguridad. Figura como objeto el de " *establecer las normas de actuación del personal encargado de la custodia de detenidos …con objeto de garantizar los derechos de los detenidos y la seguridad de los mismos y del personal policial*."

"*Las grabaciones serán conservadas durante treinta días a partir de su captación. Una vez finalizado dicho plazo serán destruidas, salvo que se produzca algún incidente en el transcurso de la custodia de un detenido o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública; con una investigación policial en curso o con un procedimiento judicial o administrativo abierto. En estos casos, la grabación se conservará a disposición de las Autoridades competentes*."

A diferencia de la anterior instrucción, en esta no se indica que los sistemas de videovigilancia se regirán por lo que establece la Ley Orgánica 4/1997, de 4/08, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de seguridad en lugares públicos.

4) En el periodo de pruebas, además se indica por la propia Comisaria de ******LOCALIDAD.1*** que dispone de cámaras para la seguridad de la comisaria y protección interior y exterior del edificio y en el Informe de la Subdirección General de Logística e Innovación de 3/12/2018, destinatario "delegado de protección de datos. Gabinete Técnico" se precisa que estas cámaras son para la "finalidad de "*garantizar la protección interior y exterior de las Comisarias del CNP y de los edificios, instalaciones y centros vigilados por el mismo.* Su uso está dirigido a la "*seguridad y protección*". A este sistema se le aplica la LOPD, de acuerdo con la orden de creación de ficheros- Orden INT/1202/2011, de 4/05, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, BOE 12/12/2016

5) La reclamada no ha concretado, al no responder en pruebas, con qué tipo de cámara se obtuvieron las imágenes sobre el cumplimiento de la uniformidad por el reclamante, en que espacios se tomaron, a cuál de los dos sistemas corresponde (vigilancia de celdas o de la comisaria en general) y que protocolo existe de petición de imágenes y entrega.

6) Ninguna de las finalidades del tratamiento de la recogida de datos los dos sistemas, de videovigilancia contemplan el uso de sus imágenes con fines de verificación de conductas, de cumplimiento del régimen interior, o de faltas disciplinarias que pudieran cometer los agentes, que fue la finalidad de la petición y extracción de las del reclamante la noche del ******FECHA.2***.

7) Además, se acredita que la petición de imagen y su entrega al Inspector ******PUESTO.2***, superior del reclamante no está, ni figura en protocolo alguno que regule la cuestión, debiendo tener acceso a las imágenes exclusivamente las personas autorizadas expresamente en algún tipo de documento o protocolo que regule la solicitud de imágenes, motivos y documentación de esos aspectos.

8) No se acredita que se haya iniciado o resuelto procedimiento disciplinario contra el reclamante o en base a la falta de uniformidad de la noche del ******FECHA.1***, aunque si la petición de las imágenes y su entrega.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 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 es-

tos datos (en lo sucesivo, RGPD); reconoce a cada autoridad de control, y según lo establecido en el art. 47 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), la directora de la AEPD es competente para iniciar y para resolver este procedimiento.

II

En el presente supuesto, dada la falta de concreción de la reclamada, al no precisar con qué tipo de cámara ni su ubicación o régimen se captan las imágenes que comunica el reclamante, se puede deducir que pudiera haber dos tipos de cámaras en la Comisaria donde suceden los hechos. El resultado es que cualquiera que hubiese sido el sistema de cámaras empleado, la extracción por los motivos que se produjo y directamente por el primer superior del reclamante, vulnera el RGPD en cuanto a que no se contempla en ninguno de los dos sistemas el uso de reprensión de conductas irregulares por parte de los Agentes, y además no aparece regulado en su caso quien ha de pedir las imágenes.

Por un lado, las cámaras que vigilan las celdas de los detenidos, con su régimen aplicable de la **Ley Orgánica ****LEY.1*** por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, precisa una autorización previa emisión de un informe por un órgano colegiado, y la "*resolución por la que se acuerde la autorización deberá ser motivada y referida en cada caso al lugar público concreto que ha de ser objeto de observación por las videocámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes. Asimismo, deberá precisar genéricamente el ámbito físico susceptible de ser grabado, el tipo de cámara, sus especificaciones técnicas y la duración de la autorización, que tendrá una vigencia máxima de un año, a cuyo término habrá de solicitarse su renovación*."

Como criterios de autorización para tener en cuenta se indican: "*Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes*." Art 4

En su artículo 6 se reseñan los "*principios de utilización de las videocámaras:*

1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.

2. La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

3. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

4. La utilización de videocámaras exigirá la existencia de un razonable riesgo para la

seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia.

El espacio que han de enfocar dichas cámaras está relacionado con la obligatoriedad de la existencia de cámaras de videovigilancia para observar y garantizar la seguridad de los detenidos en calabozos policiales. Dicha modalidad relacionada con la seguridad pública no parece directamente relacionada con la falta de uniformidad del empleado público reclamante, que manifiesta, al ser la noche de ******FECHA.1*** que ante el intenso frío que existe en dicha Comisaria, portaba un forro polar sobre el uniforme.

Por tanto, por razón de la materia, ni las que tienen como finalidad la vigilancia de los detenidos en celdas, ni las que haya instaladas en la comisaria, a las que se les aplica la LOPD, desde mayo 2018 el RGPD, son susceptibles de ser utilizadas con el fin para el que lo han sido, sin haberse pre informado de dicha finalidad. Para ello, antes se debería haber decidido por el responsable del tratamiento, que el seguimiento de las eventuales conductas susceptibles de ser disciplinadas a través de dicho medio y modalidad de videovigilancia para los agentes en la comisaria se acometiera con estos medios, cuestión que afecta a sus derechos laborales y su intimidad y habría que valorar la proporcionalidad e idoneidad del sistema, o para que supuestos.

La Instrucción 1/201/2006, de 8/11 de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, BOE 12/12 indicaba en su preámbulo:

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

Ante la falta de aclaración por la reclamada del tipo de cámaras con el que se obtuvieron las imágenes, nada aportó a lo solicitado en pruebas, se debe indicar que el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la

estricta observancia del principio de proporcionalidad».

Su artículo 4 indica:

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras."

Señala el artículo 1 del RGPD "*El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.*

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales."

El art. 4.1 y . 2 del RGPD indica *"*1*) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

2) *«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;*

El sistema de videovigilancia en el presente supuesto supone una identificación directa de la persona cuyas acciones son recogidas al hallarse en su espacio de grabación. En este caso en la Comisaria había dos sistemas distintos implantados el de videovigilancia para las celdas de detenidos y el general para seguridad de las instalaciones, siendo la finalidad diferente, por lo demás ninguno de ellos para la finalidad de comprobación de conductas o represión de infracciones de los agentes.

En este caso se consideran datos de carácter personal, la fisonomía del Agente, identificable, junto a su vestimenta, relacionando si el reclamante había adecuado la misma vestimenta al reglamento interno de personal, captándose a modo de acreditación fehaciente la obtención de las imágenes que enfocaban ese espacio entre un tramo diferenciado horario, que fue seleccionado por el ******PUESTO.2***, que horas antes le había visto y advertido de la falta de uniformidad, al objeto de sancionar una falta.

El uso de las imágenes en ambos sistemas, grabación, conservación, extracción, se relaciona con seguridad de las personas, los agentes o instalaciones. Sin embargo, en este caso se han utilizado en el ámbito laboral como medio de comprobación. La AEPD no se pronuncia sobre la validez de las imágenes que se aportaran al procedimiento disciplinario, sino por la legitimidad y legalidad del mismo conforme a la normativa de protección de datos y el tratamiento que se acredita se lleva a cabo con los datos personales del afectado.

El artículo 18.4 de la Constitución española indica: "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

De acuerdo con la sentencia del Tribunal Constitucional 254/1993 que inicia la doctrina del derecho de protección de datos: *"…De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos."*

Como conclusión de los dos informes del Gabinete Jurídico de la AEPD alegados por la reclamada, no cabe colegir que las cámaras de videovigilancia para control interno situadas en las Comisarias, sean de control de entradas, sean de otro tipo, al que no se refieren los informes, en cuanto a que su fin sea la seguridad de sus instalaciones y su personal, no cabe un uso extensivo para fines de corrección de conductas disciplinarias de sus empleados, sean Agentes de policía, sea otro tipo de personal, como la de control del uniforme del reclamante. Con dicho tratamiento de datos para ese fin disciplinario, se afecta a la esfera jurídica de su personal, creándose un medio de verificación de cumplimiento de conductas sin la información previa que afecta a un derecho fundamental, sin seguridad jurídica alguna en cuanto a su uso, sujetos habilitados para la petición, exacción, y derechos del afectado de acceso, cancelación, conservación y no manipulación, seguridad, etc.

Tampoco es cierto que con la LOPD se habilitasen usos distintos a la finalidad propia del fichero o tratamiento. Además, se recuerda que no se sanciona el uso incompatible, sino un uso para una finalidad para la que no se informó, ajeno a las expectativas de los empleados.

III

El RGPD, artículo 5.1.b) del RGPD indica:

"1. Los datos personales serán:

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)

Requisito para que un tratamiento de datos sea conforme a lo establecido en la normativa es que el mismo se encuentre legitimado en lo previsto en su artículo 6 y que se ajuste a sus principios del artículo 5. Ahora bien, no cabe legitimar el tratamiento de datos de videovigilancia para fines de verificación de cumplimiento del reglamento interno en el consentimiento de los empleados. Para ello, habrá que acudir a otra base legitima que podría ser el control del cumplimiento de las obligaciones jurídicas establecidas, pero como se ha apuntado anteriormente ello exigiría valorar diversos elementos y tener en cuenta diversos aspectos, entre otros la proporcionalidad de uso, en este caso de una orden que se dio al ver al Agente que no iba correctamente uniformado, para que lo hiciera.

En este caso, las imágenes son tratadas con un fin que no es el previsto por las operaciones de tratamiento instauradas por los sistemas de videovigilancia de la Comisaria.

Se aplique la LOPD, o se aplique el RGPD, el principio básico incumplido, caso de que el sistema se considerase proporcional a los fines y se hubiera implantado, es que no se informó a los afectados, en este caso al reclamante, de la utilización del sistema, de sus consecuencias y de los derechos que se derivan del mismo. La circunstancia de no haberse hecho supone, con su uso, un desvió de finalidad, pues el sistema estaba contemplado para fines de seguridad de la Comisaria, de los Agentes, o en su caso, de los detenidos. El principio incumplido es por el que se abre la infracción a la reclamada, 5.1 b) del RGPD.

Por otro lado, las consecuencias en ambas normas es la declaración de infracción LOPD o el apercibimiento, RGPD. En ambos casos supone la declaración de una forma de actuar no concorde con la normativa de protección de datos y el requerimiento para adecuación de conductas en lo sucesivo, si no se ha hecho durante la sustanciación del mismo a lo que la norma prevé.

En este sentido, se ignora si se ha utilizado con posterioridad el sistema de videovigilancia en algún supuesto similar al denunciado en dicha comisaria, dada la falta de explicaciones a lo solicitado en pruebas.

IV

Además, para la virtualidad del funcionamiento del sistema, sería necesario el cumplimiento del principio, que impone la obligación de información previa a los empleados y la consulta a sus representantes. En tal sentido, merece atención mencionar la sentencia del Tribunal Constitucional de 29/2013 de 11/02 que en un caso de control por videovigilancia de un empleado de la Universidad de Sevilla del que existía la sospecha de irregularidades en el cumplimiento de su jornada laboral, en su fundamento de derecho VII indicaba:

"Ese derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento. Es verdad que esa exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas, pero no debe olvidarse que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental, exigiendo además que el recorte que experimenten sea necesario para lograr

el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2, y en relación con el derecho a la protección de datos personales, STC 292/2000 [RTC 2000, 292] , FF. 11 y 16).”

No existe una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de los datos personales en el ámbito de las relaciones laborales, sin que a tal efecto baste como fundamento el interés de controlar la actividad, y sin que tampoco sea suficiente que, en el caso concreto, ese tratamiento de datos resulte eventualmente proporcionado al fin perseguido.

El TCo, 29/2013 añadió que era necesaria una información «*previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida» y que «debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo*».

La idea de la que se debe partir al determinar el contenido esencial del derecho que consagra el artículo 18.4 de la CE es que si la legislación reconoce unas determinadas garantías vinculadas al derecho fundamental a la protección de datos de carácter personal, en este caso, se deberá respetar el deber informativo previo que permita tener cabal conocimiento de quién posee los datos personales y para qué se utilizan. Sólo así podrá el trabajador o empleado conocer del uso y consecuencias de la recogida de sus datos, “*autodeterminación informativa*”, y solicitar además, como parte de su derecho, la limitación, acceso, cancelación o supresión de los datos.

En este caso, al extracción concreta y puntual, predeterminada de una franja horaria en que el reclamante no estaba uniformado, ha servido de forma directa para controlar el cumplimiento de su uniformidad con un sistema de videovigilancia que no tenía esa finalidad.

V

El artículo 58.2 b) y d) del RGPD dispone lo siguiente: “Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

b) 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;

La imposición de esta medida es compatible con la sanción de apercibimiento, según lo dispuesto en el art. 83.2 del RGPD.

No se imponen medidas concretas a implementar por la reclamada, dado que no aparece detallado el tratamiento con la finalidad con que ha sido llevado a cabo, debiendo

no volverse a utilizar en otra ocasión, a menos que acredite la proporcionalidad de la finalidad del uso de verificación de la reglamentación disciplinaria y la adecuada y clara información sobre dicho uso a los afectados. Como se ha indicado en esta resolución, tendría que añadirse una nueva finalidad si decidiera llevar a cabo el control disciplinario por el sistema de captación de videocámaras en el interior de las comisarias, para lo que debería cumplir los requisitos del RGPD.

El artículo 83.5.a) del RGPD indica

"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;"

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*"

La LOPDGDD, en su artículo 77 indica

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

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."

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

PRIMERO: IMPONER una sanción de APERCIBIMIENTO a la **DIRECCION GENERAL DE LA POLICIA (MINISTERIO DEL INTERIOR)**, con NIF **S2816015H**, por una infracción del Artículo 5.1 b) del RGPD, de conformidad con el Artículo 83.5 y 58.2.b) del RGPD.
/

SEGUNDO: NOTIFICAR la presente resolución a la **DIRECCION GENERAL DE LA POLICIA (MINISTERIO DEL INTERIOR)**.

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

CUARTO: 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 13/07, 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 1/10. 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