

Procedimiento N°: PS/00345/2020RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: Con fecha 29 de junio de 2020, tuvo entrada en esta Agencia Española de Protección de Datos un escrito presentado por Don **A.A.A.** (*en lo sucesivo, el reclamante) y otro, mediante el que formula reclamación contra *****COMUNIDAD.1** con NIF *****NIF.1*** (en adelante, el reclamado), por la instalación de un sistema de videovigilancia instalado en *****URBANIZACIÓN.1**, *****DIRECCIÓN.1**, existiendo indicios de un posible incumplimiento de lo dispuesto en la normativa de protección de datos.

Los motivos que fundamentan la reclamación son los siguientes;

“[...] Que según puede apreciarse en las fotos y documentación anexas a este escrito existen las siguientes cámaras de seguridad situadas en espacios peatonales, zonas comunes como piscinas y zonas de trabajo:

1º En el interior de las garitas de la comunidad de propietarios, se han instalado 2 cámaras de videovigilancia, una en cada garita de seguridad con opción a sonido, dichas cámaras carecen de cartel avisador obligatorio, en este lugar es donde nos vestimos y es nuestro comedor ya que carecemos de instalaciones aparte como vestuario y zona de descanso para comer [...].

Aparte estas cámaras que instalan en el interior de las garitas tienen audio, violando así nuestros derechos a la intimidad y secreto de las comunicaciones, [...]

Adjunto cuadrantes de los trabajadores que aparecemos en las fotos adjuntas, para que puedan verificar así los hechos relatados como turnos de trabajo, horarios en los que somos grabados sin nuestro consentimiento etc., ya que no se nos ha informado de que íbamos a ser grabados, les informo que hay una denuncia interpuesta ante la inspección de trabajo [...] y les informo también que existe una inspección por parte de la policía nacional de Málaga, departamento de seguridad privada CON FECHA 19-FEBRERO.2020, [...], las actas de inspección de los agentes verifican parte de los hechos relatados.

2º Que hay cámara apuntando hacia la piscina, donde recogen imágenes de las mismas y de los usuarios, violando así el derecho a la intimidad y al honor de las personas y de la del menor.

3º Que por la urbanización hay colocación de cámaras de videovigilancia, de las cuales varias de ellas van equipadas con un mecanismo de recogida de audio, careciendo de carteles avisadores.

4º Que las cámaras de las entradas a la urbanización, visualiza parte de la vía pública, como viales, aceras, pasos de peatones los cuales dichas instalaciones mencionadas son ajenas a la urbanización [...].

5º La empresa que ha montado las cámaras, al parecer carece de los permisos pertinentes para el montaje de cámaras de videovigilancia [...]

6º Que en toda la urbanización carece de carteles avisadores de la instalación de videovigilancia [...], quién es el responsable del fichero de datos [...]

[...] ni dirección ni persona ante la que poder ejercer los derechos ARCO.

Que no consta la existencia de documento de seguridad alguno que regule, entre otros aspectos, las funciones y responsabilidades de quienes ejerzan el tratamiento de los datos registrados.

[...]”

Adjunta un reportaje fotográfico de cámaras interiores y exteriores y cuadrantes de turnos de trabajo de los reclamantes.

SEGUNDO: Con carácter previo a la admisión a trámite de esta reclamación, la Subdirección General de Inspección de Datos dirigió, el día 10 de julio de 2020, una solicitud de información al reclamado en el que se le comunicaba que la Agencia de Protección de Datos había tenido conocimiento de la existencia de cámaras de videovigilancia situadas en la dirección indicada en el hecho primero que podrían estar vulnerando la normativa de protección de datos y en el que se le solicitaba que, en el plazo de un mes, acreditase la conformidad de la mencionada instalación con la citada normativa

Ante el rechazo de la notificación electrónica por haber transcurridos diez días desde su puesta a disposición, se reiteró una nueva solicitud de información el día 23 de julio de 2020 por correo postal. En esta reiteración se recordaba al reclamado que, en cumplimiento del artículo 14.2 de la ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), las personas jurídicas y las entidades sin personalidad jurídica, así como quienes representen a sujetos obligados, entre otros, estarán obligados a relacionarse con las Administraciones Públicas a través de medios electrónicos. La notificación de la reiteración fue devuelta por Sobrante (no retirado en oficina) el día 10 de agosto de 2020

Una segunda reiteración de la solicitud de información fue realizada el 13 de agosto de 2020, siendo devuelta nuevamente por Sobrante (no retirado en oficina) el día 11 de septiembre.

TERCERO: La reclamación fue admitida a trámite mediante resolución de 29 de septiembre de 2020.

CUARTO: El día 22 de abril de 2021 tiene entrada en el Registro de la Agencia Española de Protección de Datos escrito del reclamante con el siguiente contenido:

“Se admita como prueba los informes de la Inspección de Trabajo que se adjunta a este escrito y cuyo expediente ya se notificó en la denuncia que interpusimos, y se admita como prueba la inspección realizada por la unidad territorial del Cuerpo Nacional de Policía Unidad de Seguridad Privada la cual adjuntamos a este escrito, donde se refleja en la actuación de los agentes, de que se está grabando la vía pública.

En dichos informes, podrán comprobar la veracidad de los hechos denunciados por nuestras personas ante esta Agencia, y solicitamos que se tenga en cuenta a la presidenta de la comunidad denunciada, Doña [...] con domicilio [...] como persona no autorizada para visualizar en directo desde su teléfono móvil personal y desde su ordenador personal las cámaras de videovigilancia que venimos denunciando, y así lo confirma el informe de la Inspección de Trabajo que se les adjunta. [...]”

Se acompaña a este escrito las páginas 1, 2 y 3 del informe de actuaciones de la Inspección de Trabajo (fecha de registro de salida 08/04/2021) y el informe de la Policía Nacional.

QUINTO: Con fecha 18 de junio de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del Artículo 32 del RGPD, Artículo 5.1.c) del RGPD, tipificada en el Artículo 83.5 del RGPD.

SEXTO: En fecha 13/05/21 se procede a notificar el cambio de Instructor (a) del presente procedimiento. Constando como “Notificado” en el sistema informático de esta Agencia.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS

Primero. Los hechos traen causa de la reclamación de fecha 29/06/20 por medio de la cual se denuncia la presencia de diversas cámaras “en espacios peatonales, zonas comunes (como piscinas y zonas de trabajo)” –folio nº 1--.

Segundo. Consta identificado como principal responsable ***URBANIZACIÓN.1(...)

Tercero. Consta acreditada la presencia de cámaras de video-vigilancia en el interior de las Garitas dónde los reclamantes proceden a cambiarse, sin que exista otro lugar habilitado a tal efecto, careciendo las mismas de cartel informativo informando de su presencia.

Cuarto. Consta acreditado que el/la Presidenta tiene acceso al contenido de las grabaciones a través de su dispositivo móvil.

Quinto. No es posible determinar una captación excesiva de espacio público en virtud de las pruebas disponibles en el presente procedimiento sancionador.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

El artículo 63.2 de la LOPDGDD determina que: *«Los procedimientos tramitados por la Agencia Española de Protección de Datos se registrarán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.»*

II

La imagen física de una persona, a tenor del artículo 4.1 del RGPD, es un dato personal y su protección, por tanto, es objeto de dicho Reglamento. En el artículo 4.2 del RGPD se define el concepto de “tratamiento” de datos personales.

Es, por tanto, pertinente analizar si el tratamiento de datos personales (imagen de las personas físicas) llevado a cabo a través del sistema de videovigilancia denunciado es acorde con lo establecido en el RGPD.

III

El artículo 6.1 del RGPD establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

Por su parte, el artículo 5.1.c) del RGPD, relativo a los principios del tratamiento, dispone que los datos personales serán *“adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (“minimización de datos”).* Este artículo consagra el principio de minimización de datos en el tratamiento de los datos personales. Supone que dicho tratamiento sea ajustado y proporcional a la finalidad a la que se dirige, debiendo restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de los mismos.

La pertinencia en el tratamiento de los datos debe producirse tanto en el ámbito de la recogida de los datos como en el posterior tratamiento que se realice de los mismos.

Por su parte, el artículo 22 de la LOPDGDD, cuya rúbrica es “Tratamientos con fines de videovigilancia” establece que:

“1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la fina-

lidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.”

IV

De conformidad con lo expuesto, el tratamiento de imágenes a través de un sistema de videovigilancia, para ser conforme con la normativa vigente, debe cumplir los requisitos siguientes:

- Respetar el principio de proporcionalidad.
- Las videocámaras no podrán captar imágenes de las personas que se encuentren fuera del espacio privado en donde esté instalado el sistema de videovigilancia, ya que el tratamiento de imágenes en lugares públicos sólo puede ser realizado, salvo que concurra autorización gubernativa, por las Fuerzas y Cuerpos de Seguridad. Tampoco pueden captarse ni grabarse espacios propiedad de terceros sin el consentimiento de sus titulares, o, en su caso, de las personas que en ellos se encuentren.

Esta regla admite alguna excepción ya que, en algunas ocasiones, para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública. Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas y extraordinariamente también se recogerá el espacio mínimo para dicha finalidad. Por lo tanto, las cámaras podrían excepcionalmente captar la porción mínimamente necesaria para la finalidad de seguridad que se pretende.

- Se deberá cumplir el deber de informar a los afectados previsto en los artículos 12 y 13 del RGPD y 22.4 de la LOPDGDD.

En concreto se deberá colocar en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados, en el que se identificará, al menos, la existencia de un tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en dichos preceptos. Asimismo, deberá mantenerse a disposición de los afectados la información a la que se refiere el citado RGPD.

- El responsable deberá llevar un registro de actividades de los tratamientos efectuados bajo su responsabilidad en el que se incluya la información a la que hace referencia el artículo 30.1 del RGPD.

- Las cámaras instaladas no pueden obtener imágenes de espacio privativo de tercero y/o espacio público sin causa justificada debidamente acreditada, ni pueden afectar a la intimidad de transeúntes que transiten libremente por la zona. No está permitida, por tanto, la colocación de cámaras hacia la propiedad privada de vecinos con la finalidad de intimidarlos o afectar a su ámbito privado sin causa justificada.

- En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular, no pudiendo afectar a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.
- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.
- Las imágenes que se utilicen para denunciar delitos o infracciones se acompañarán a la denuncia y serán conservadas para ser entregadas a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que lo requieran. No podrán utilizarse para otro fin.
- La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a su titular del cumplimiento del RGPD.
- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que reúna los requisitos contemplados en el artículo 5 de la Ley 5/2014 de Seguridad Privada, de 4 de abril.

En relación con lo expuesto, para facilitar la consulta a los interesados la Agencia Española de Protección de Datos ofrece a través de su página web [<https://www.aepd.es>] acceso a la legislación en materia de protección de datos personales, incluyendo el RGPD y la LOPDGDD (apartado “Informes y resoluciones” / “normativa”), así como a la Guía sobre el uso de videocámaras para seguridad y otras finalidades, así como la Guía para el cumplimiento del deber de informar (ambas disponibles en el apartado “Guías y herramientas”).

También resulta de interés, en caso de realizar tratamientos de datos de bajo riesgo, la herramienta gratuita Facilita (en el apartado “Guías y herramientas”), que mediante unas preguntas concretas, permite valorar la situación del responsable respecto del tratamiento de datos personales que lleva a cabo, y en su caso, generar diversos documentos, cláusulas informativas y contractuales, así como un anexo con medidas de seguridad orientativas consideradas mínimas.

En los supuestos en que el sistema de videovigilancia capte imágenes en zonas o elementos comunes de una comunidad de propietarios, además de los requisitos generales anteriores se deberá tener en cuenta lo siguiente:

- Será necesaria la existencia de un acuerdo de la Junta de la Comunidad de Propietarios en los términos que establece la Ley 49/1960, de 21 de julio, sobre propiedad horizontal (en adelante, LPH).
- Si está prevista la instalación de cámaras en la zona de la piscina comunitaria, el acuerdo de la Junta de la Comunidad de Propietarios deberá autorizar en concreto dichas cámaras.

- No podrán captarse imágenes de la vía pública a excepción de una franja mínima de los accesos al inmueble, ni tampoco imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno.
- El acceso a las imágenes y a las grabaciones estará restringido a las personas designadas por la comunidad.
- En ningún caso estarán accesibles a los vecinos mediante canal de televisión comunitaria.

V

La reclamación se basa en la “presunta” ilicitud de la instalación por parte del reclamado de:

☐ Una cámara en el interior de cada garita de seguridad de la *****URBANIZACIÓN.1, ***DIRECCIÓN.1.**

sin tener en cuenta que estas instalaciones se usan como vestuario y zona de descanso por los trabajadores. Estas cámaras carecen de dispositivo informativo y podrían estar captando audio.

☐ Las cámaras instaladas en el interior de la urbanización carecen de cartel informativo y podrían estar captando asimismo audio.

☐ Por último, las cámaras ubicadas en los accesos a la urbanización estarían captando vía pública de manera desproporcionada y carecerían de cartel informativo.

Como prueba de estas manifestaciones, el reclamante aportó las evidencias señaladas en el apartado de “Hechos”, primer y cuarto punto, de este acuerdo.

De acuerdo con la reclamación y lo que es posible visualizar en el reportaje fotográfico anexo a la misma (ya que algunas de las fotografías son borrosas) y en los informes aportados (el informe de la Policía Nacional – Unidad de Seguridad Privada es ilegible), se puede observar la existencia de una cámara instalada en la parte superior de un espacio anterior y en imágenes ampliadas de lo visionado por los monitores, se consigue discernir la imagen del interior de las garitas con los trabajadores en su interior. De lo observado en estas imágenes y de lo puesto de manifiesto en el informe de la Inspección de Trabajo, se desprenden evidencias de que el sistema de videovigilancia instalado en las garitas, con independencia de no haber sido incluidas (de acuerdo con el informe mencionado) dentro de las cámaras objeto de la autorización acordada por la Comunidad de Propietarios —en la Junta General Extraordinaria de 19 de noviembre de 2019— en cumplimiento de la LPH, podría estar vulnerando el principio de minimización de datos.

☐ El artículo 22.1 de la LOPDGDD dispone que *“las personas podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones”* dedicándose el resto de los apartados de este artículo a las especificidades a las que deberá someterse este tratamiento de datos.

□ Por lo que se refiere a la proporcionalidad de la medida, las cámaras instaladas, aunque no tengan habilitado el audio, estarían captando unas zonas que se encuentran habilitadas además de como lugar de trabajo, como lugar de descanso donde los trabajadores pertenecientes a la empresa de vigilancia pueden realizar las pausas del trabajo. Estas cámaras estarían captando, por lo tanto, aspectos pertenecientes a la esfera privada de las personas que trabajan en ellas, algo que se considera desproporcionado por el nivel de intrusión en la intimidad que esto supone.

Por otra parte, aunque en este caso no es posible determinarlo claramente por cuanto no se observan nítidamente las fotografías, se recuerda que, de acuerdo con el artículo 22.2 de la LOPDGDD solo se podrá captar vía pública en el mínimo imprescindible para garantizar el perímetro y los accesos a la urbanización. Abundando en esta cuestión, se informa de que la facultad de captar imágenes en vía pública está atribuida, con carácter general, a las Fuerzas y Cuerpos de Seguridad de conformidad con lo dispuesto en la Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su normativa de desarrollo.

Asimismo, aunque tampoco se puede determinar, se recuerda la existencia de proporcionar información. De acuerdo con el artículo 22.6 de la LOPDGDD, este deber se entenderá cumplido con la colocación de un dispositivo informativo que recoja el tratamiento que se lleva a cabo, la identidad del responsable y la posibilidad de que por parte del interesado se puedan ejercitar los derechos recogidos en los artículos 15 a 22 del RGPD. Todo ello sin perjuicio de que por el responsable se mantenga el resto de la información a disposición de los afectados.

Por último, se significa que las Comunidades de Propietarios pueden acordar la instalación de cámaras orientadas hacia las piscinas en la forma establecida en la LPH, debiendo autorizarse dichas cámaras de manera expresa.

VI

En otro orden de cosas, es necesario señalar que artículo 5 del RGPD, cuya rúbrica lleva por título *Principios relativos al tratamiento* establece en la letra f) de su apartado 1 que los datos personales serán *“tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (“integridad y confidencialidad”)*”, cuestión sobre la que también se refiere el artículo 5 de la LOPDGDD.

En relación con las medidas mencionadas en el artículo 5.1.f) del RGPD antes transcrito, el artículo 32 de la misma norma dispone que:

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.”

En relación con un adecuado cumplimiento de las medidas de seguridad en el ámbito de los tratamientos llevados a cabo por los sistemas de videovigilancia, el responsable vendrá obligado a adoptar las medidas técnicas necesarias en orden a garantizar la seguridad, confidencialidad y el acceso no autorizado a las imágenes. El hecho de que la presidenta de la Comunidad de Propietarios tenga acceso a la visualización en directo de imágenes de las cámaras de videovigilancia en dispositivos de uso personal podría suponer un riesgo para la seguridad y confidencialidad de los datos.

VII

Los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, se establecen en el artículo 58.2 del RGPD. Entre ellos se encuentran la potestad de dirigir un apercibimiento -artículo 58.2 b)-, la potestad de imponer una multa administrativa con arreglo al artículo 83 del RGPD -artículo 58.2 i)-, o la potestad de ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado -artículo 58. 2 d)-.

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en el artículo 58.2 d) del citado Reglamento es compatible con la sanción consistente en multa administrativa.

Sin perjuicio de lo establecido en el artículo 83 del RGPD, el citado Reglamento dispone en su art. 58.2 b) la posibilidad de dirigir un apercibimiento, en relación con lo señalado en el Considerando 148:

“En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante.”

VIII

De conformidad con las evidencias de las que se dispone en el presente procedimiento sancionador, se considera que los hechos expuestos incumplen lo establecido en el artículo 5.1.c) del RGPD.

Para entender mejor la legislación sobre la utilización de cámaras de videovigilancia o seguridad, tenemos que irnos al artículo 20.3 del Estatuto de los Trabajadores. Dicho artículo señala que los empresarios pueden adoptar las medidas de control que consideren necesarias para garantizar el cumplimiento de la normativa dentro de sus instalaciones, lo cual incluye la instalación de cámaras de seguridad.

El empresario no puede ejercer este derecho de forma unilateral, sino que debe cumplir una serie de requisitos. El primero de ellos es el **deber de informar** a todos los interesados sobre la instalación de las cámaras, por ejemplo, colocando un cartel indicando que es una zona videovigilada.

Otros aspectos que se han de tener en cuenta son la proporcionalidad y el respeto a la intimidad e integridad de los trabajadores. En este sentido, la instalación de cámaras de seguridad siempre deberá responder al principio de proporcionalidad, es decir, que el uso de las cámaras de seguridad sea proporcional al fin perseguido, esto es garantizar la seguridad y el cumplimiento de las normas.

Por consiguiente, la presencia de una cámara (s) en la Garita de seguridad no parece una medida idónea, si la misma es utilizada simultáneamente como cuarto de vestuario, al afectar a la intimidad de los trabajadores (as), con independencia de que se pudiera establecer la obligatoriedad de que la presencia en el puesto de trabajo se realizase uniformada, decisión esta en su caso de la Comunidad de propietarios en su condición de empleador.

Lo anterior supone una infracción tipificada en el artículo 83.5 del RGPD, que dispone lo siguiente:

“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; [...]”.

A efectos del plazo de prescripción de las infracciones, las señaladas en el párrafo anterior se consideran muy grave y prescriben a los tres años, conforme al artículo 72.1 de la LOPDGDD, que establece que:

“En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.

Asimismo, se estaría vulnerando el artículo 32 del RGPD, infracción tipificada como grave en el artículo 83.4:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; [...]”

A efectos del plazo de prescripción de las infracciones, esta infracción se considera grave y prescribe a los dos años, conforme al 73 de la LOPDGDD, que establece que:

“En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

[...] f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679. [...]”

IX

Por la infracción del artículo 5.1.c) se considera que la sanción adecuada es la de multa administrativa. A este respecto, la multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Por tanto, procede graduar la sanción a imponer de acuerdo con los

criterios que establece el artículo 83.2 del RGPD, y con lo dispuesto en el artículo 76 de la LOPDGDD, respecto al apartado k) del citado artículo 83.2 RGPD.

En el presente caso, se han tenido en cuenta en la valoración inicial los siguientes elementos:

☐ Como circunstancia agravante, se toma en consideración la de intencionalidad o negligencia en la infracción (artículo 83.2.b) del RGPD) por cuanto el responsable no puede desconocer que en relación con los fines de seguridad de la comunidad el alcance de las cámaras instaladas en las garitas se refiere únicamente a su interior, así como su uso como lugar de descanso de los trabajadores de la empresa.

☐ Como circunstancias atenuantes, se consideran concurrentes las siguientes:

1. Que se trata de una entidad cuya actividad principal no está vinculada con el tratamiento de datos personales.

2. que no se aprecia reincidencia, por no constar la comisión, en el término de un año, de más de una infracción de la misma naturaleza.

Por todo ello, se considera que la sanción que correspondería imponer sería la siguiente:

-Por la infracción del artículo 5.1.c), una multa de **mil euros** (1.000,00 €).

-Por la infracción del artículo 32 del RGPD, se considera, que concurren las circunstancias atenuantes descritas anteriormente, por lo que se considera adecuado dirigir un **apercibimiento**.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

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

PRIMERO: IMPONER a *****COMUNIDAD.1**, con NIF *****NIF.1**, por una infracción del Artículo 5.1.c) del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de **1000€** (Mil euros).

SEGUNDO: DIRIGIR un apercibimiento a la entidad *****COMUNIDAD.1**, con NIF *****NIF.1**, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD.

TERCERO: ORDENAR a *****COMUNIDAD.1** para que en el plazo de 1 mes desde la notificación del presente acto administrativo proceda a adecuar los tratamientos de da-

tos realizados a la normativa de protección de datos; en particular que quiten las cámaras de los espacios que obtienen una grabación desproporcionada y que incorporen las medidas de seguridad que eviten accesos indebidos a imágenes.

CUARTO: NOTIFICAR la presente resolución a *****COMUNIDAD.1**.

QUINTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria **CAIXABANK, S.A.**. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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

938-131120